Loyola University Chicago Law Journal

Volume 28
Issue 1 *Fall 1996*

Article 6

1996

Changing Technologies and the Expectation of Privacy: A Modern Dilemma

Michelle Skatoff Gee

Comment

Changing Technologies and the Expectation of Privacy: A Modern Dilemma

I. INTRODUCTION

In March, 1996, government officials arrested a twenty-one year old Argentine computer hacker who illegally accessed U.S. military computers by tapping into Harvard University's computer system.[1] A court-ordered wiretap enabled the arrest by permitting investigators to conduct a computerized surveillance of the 60,000 electronic mail messages transmitted daily over the Harvard system.[2] Investigators designed a surveillance method to ignore irrelevant electronic mail communications.[3] During the two month wiretap, investigators inadvertently read only a couple of irrelevant communications.[4] Attorney General Janet Reno touted this successful investigation as "an example of how the 4th Amendment . . . and a court order can be used to protect rights while adapting to modern technology."[5]

Attorney General Reno's statement evokes the tension between three primary concerns of the present-day wiretap debate: (1) the government's need to investigate crimes; (2) an individual's constitutional rights; and (3) the changing nature of communication technologies.[6]

---

1. Linnet Myers, *Cybersleuthing vs. Civil Rights: Hacker Identified after Network is Wiretapped*, CHI. TRIB., Mar. 30, 1996, at 1. The 21 year old Buenos Aires student used stolen passwords to tap into Harvard University's computer system and thereby gain access to U.S. military records, including those at NASA's Jet Propulsion Laboratory and the Los Alamos National Laboratory. *Id.* Although the student never uncovered top-secret data, he faces criminal charges, including fraudulent possession of unauthorized computer passwords and user identification names. *Id.*

2. *First Internet Wiretap Leads to a Suspect*, N.Y. TIMES, Mar. 31, 1996, at 20.

3. Myers, *supra* note 1, at 10.

4. *Id.*

5. *First Internet Wiretap Leads to a Suspect, supra* note 2, at 20.

6. Advancements in technology increase the possibilities for invasions of privacy as the constitutional definition of an individuals' "effects" expands. See *infra* note 12 and accompanying text for the language of the Fourth Amendment. Warrants for "wiretaps" now extend beyond tapping traditional telephone lines, to intercepting electronic mail transmissions, cellular phone transmissions, and pagers. Myers, *supra* note 1, at 1; *see also* Bob Violino & Caryn Gillooly, *Feds Tap E-Mail In Bust: Court-Approved Tactic Raises Privacy Concerns*, INFORMATION WEEK, Jan. 8, 1996, at 16 (describing federal wiretapping of electronic mail to intercept cellular phone fraud ring).

The government's ability to wiretap and intercept communications plays a central role in fighting crime.[7] Government agents use wiretaps to infiltrate drug trafficking organizations and organized crime circles, and to fight white collar crimes and terrorism.[8] The intrusive nature of government wiretaps, however, necessitates restrictions[9] on governmental eavesdropping to preserve individual privacy interests.[10] The tension between the government's need to investigate crimes and the individual's right to "be let alone"[11] comes from the language of the Fourth Amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[12]

Although the Fourth Amendment protects individual privacy to an extent, it does not forbid all intrusions.[13] Rather, the Fourth Amendment protects individuals from *unreasonable* governmental intrusions.[14] Individual rights are protected, in part, by the deterrent effect of the exclusionary rule.[15] This judicially created remedy

---

7. Geoffrey R. Greiveldinger, *Digital Telephony and Key-Escrow Encryption Initiatives: A Critical Juncture as Law Enforcement Agencies Work to Save Electronic Surveillance*, 41 FED. B. NEWS & J., Aug. 1994, at 505. From 1982 to 1992, investigations using wiretaps resulted in over 22,000 felony convictions in federal and state courts. *Id.*

8. *Id.* at 505-06.

9. *See* 18 U.S.C. § 2518 (1994) (requiring the showing of both reasonable cause and last resort for a court order authorizing or approving the interception of wire, oral or electronic communications).

10. Dalia v. United States, 441 U.S. 238, 250 n.9 (1979). The *Dalia* Court noted "Congress and this Court have recognized, however, that electronic surveillance can be a threat to the cherished privacy of law-abiding citizens unless it is subjected to the careful supervision prescribed by Title III [of the Omnibus Crime and Safe Streets Act of 1968]." *Id.* (internal quotations omitted). *See also* S. REP. NO. 541, 99th Cong., 2d Sess. 23 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

11. Justice Brandeis described the true purpose of the Fourth Amendment as protecting the "right to be let alone" by government. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). This right is "the most comprehensive of rights and the right most valued by civilized men." *Id.* (Brandeis, J., dissenting).

12. U.S. CONST. amend. IV.

13. Katz v. United States, 389 U.S. 347, 350 (1967). "[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'" *Id. But cf.* Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965) (articulating a "penumbra" theory whereby the Fourth Amendment, in conjunction with the rest of the Bill of Rights, creates a "right to privacy").

14. Berger v. New York, 388 U.S. 41, 53 (1967).

15. United States v. Turk, 526 F.2d 654, 660 (5th Cir. 1976), *cert. denied*, 429 U.S.

permits criminal defendants subject to an unreasonable governmental intrusion to move to exclude all evidence obtained from this unlawful intrusion.[16]

Before a criminal defendant can move to exclude evidence based on the exclusionary rule, however, the defendant must show that a government "search" took place.[17] Conduct amounting to a search triggers a Fourth Amendment analysis to determine whether the search was reasonable, and if so, whether the exclusionary rule can apply.[18] Until a government search occurs, government investigators are free to collect evidence in disregard of an individual's privacy.[19] Thus, a crucial factor in a Fourth Amendment analysis hinges on defining when a constitutionally protected search occurs.

This Comment first discusses the Supreme Court's evolving definition of search in conjunction with changing communication technologies.[20] This Comment then proceeds to discuss Congressional statutes that balance individuals' Fourth Amendment privacy rights with changing technology.[21] Next, this Comment considers the various judicial approaches to cases that implicate both Congressional statutes and individuals' privacy rights.[22] This

---

873 (1976).

16. Weeks v. United States, 232 U.S. 383, 398 (1914) (prohibiting use of evidence seized in violation of Fourth Amendment).

17. *Katz*, 389 U.S. at 351-53. *See also* Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (holding that no warrant was required when no search occurred).

18. John W. Hall, Jr., provides a more detailed checklist for analyzing Fourth Amendment problems. He asks:

> (1) Is the Fourth Amendment applicable to the conduct at issue? . . .
>
> (2) Is there a legally required justification (*i.e.*, probable cause or reasonable suspicion) for the intrusion? . . .
>
> (3) Does an exception to the warrant requirement apply? . . .
>
> (4) If a warrant was required, was the warrant requirement satisfied . . .
>
> (5)Whether the search was conducted with or without a warrant, was the scope of the search properly limited . . .
>
> (6) Was the search reasonable under all the circumstances? . . .
>
> (7) If the Fourth Amendment or other rules were violated, should the exclusionary rule be applied in this case?

1 JOHN W. HALL, JR., SEARCH AND SEIZURE § 1:7, at 13-14 (2d ed. 1991).

19. *See Smith*, 442 U.S. at 745.

20 *See infra* Part II.A, B.

21. *See infra* Part II.C.

22. *See infra* Part III. This Comment focuses primarily on Fourth Amendment implications associated with developing technology, such as identifying when an illegal search occurs. For a discussion of First Amendment rights implicated in internet transmissions see William S. Byassee, *Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community*, 30 WAKE FOREST L. REV. 197 (1995) (discussing problems in identifying an appropriate community standard for

Comment then determines which judicial approach successfully balances these statutes with individuals' privacy rights.[23] Finally, this Comment proposes methods for consistent statutory application and continued protection of individual privacy rights in light of changing technology.[24]

II. BACKGROUND

The Fourth Amendment protects individuals' from unreasonable searches and seizures,[25] and the Supreme Court grappled for decades with the implications of the Fourth Amendment on changing communication technologies.[26] Finally, in the 1960's, the Court settled on a two-pronged test designed to determine if a government action violated the Fourth Amendment's privacy right.[27] Because the Supreme Court inevitably falls behind changing times, however, Congress enacted a number of statutes that balance Fourth Amendment protections with modern, changing technology.[28]

A. The Judicial Progression

Prior to 1967, the Court adhered to the literal language of the Fourth Amendment to determine whether a search occurred.[29] Unless government agents searched or seized tangible "houses, papers, or effects," Fourth Amendment protections failed to apply.[30] In the 1928 case of *Olmstead v. United States*,[31] federal prohibition officers

---

pornography within the realm of the internet); *see also* Rex S. Heinke & Heather D. Rafter, *Rough Justice in Cyberspace: Liability on the Electronic Frontier*, 11 COMPUTER LAW. 1 (1994) (discussing defamation and pornography on the internet).

23. *See infra* Part IV.

24. *See infra* Part V.

25. *See infra* notes 29-64 and accompanying text.

26. *See infra* notes 29-35 and accompanying text (discussing the Fourth Amendment).

27. *See infra* notes 48-64 and accompanying text (discussing the two-prong test).

28. *See infra* notes 65-108 and accompanying text (discussing Congressional statutes).

29. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 466 (1928). The Supreme Court stated:

> Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been 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.

Id.

30. *Id.*

31. *Id.*

wiretapped phone lines to obtain evidence of a liquor importing conspiracy.[32] The officers made the wiretaps from a nearby office building without trespassing on the defendant's property.[33] A literal reading of the Fourth Amendment led a divided Court[34] to conclude that no search or seizure occurred because the officers obtained the evidence aurally, without ever entering the defendants' homes or seizing the defendants' property.[35]

Writing for the dissent in *Olmstead*, Justice Brandeis argued that this literal reading of the Fourth Amendment failed to recognize changing societal conditions.[36] He argued that the underlying principles of the Fourth Amendment must be realized, or "[r]ights declared in words might be lost in reality,"[37] as investigative technology becomes less physically intrusive.[38] Justice Brandeis urged that the underlying principle of the Fourth Amendment is simply the right to be let alone.[39] He reasoned that this right extends beyond protection from government searches of property to unjustified government intrusions of an individual's privacy.[40]

The Court eventually adopted Justice Brandeis' more expansive interpretation of the Fourth Amendment in the 1967 case of *Katz v. United States*.[41] Charles Katz was convicted of placing wagers to Miami and Boston from a telephone booth in Los Angeles, in violation of a federal statute.[42] To obtain the incriminating information, the

---

32. *Id.* at 456.

33. *Id.*

34. *Id.* at 459.

35. *Id.* at 464.

36. *Id.* at 472 (Brandeis, J., dissenting). Brandeis stated that "[c]lauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world." *Id.* (Brandeis, J., dissenting).

37. *Id.* at 473 (Brandeis, J., dissenting) (quoting Weems v. United States, 217 U.S. 349, 373 (1909)).

38. *Id.* at 474 (Brandeis, J., dissenting). *Olmstead* is often cited for Justice Brandeis' premonition that:

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?

Id. (Brandeis, J., dissenting).

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

40. *Id.* (Brandeis, J., dissenting).

41. 389 U.S. 347 (1967).

42. *Id.* at 348. Katz was convicted of violating 18 U.S.C. § 1084, which makes it a crime to "engag[e] in the business of betting or wagering [and] knowingly use[] a wire

Federal Bureau of Investigation ("FBI") listened to Katz' conversations via an electronic device attached to the exterior of the telephone booth which recorded the phone calls.[43] Rejecting the *Olmstead* requirement of a physical trespass, the Court refocused its analysis to recognize that "the Fourth Amendment protects people, not places."[44] The Court reasoned that Katz' actions of placing a call from an enclosed phone booth showed that he intended to shield his conversation from being overheard.[45] Because the FBI's eavesdropping violated the defendant's expectation of privacy, the Supreme Court held that the government's conduct constituted a "search and seizure" under the Fourth Amendment.[46] Thus, the definition of a constitutionally protected search evolved from protecting only physical invasions of property to intrusions upon an individual's "reasonable expectation of privacy."[47]

B. "Search" and the Reasonable Expectation of Privacy Threshold

Justice Harlan's concurring opinion in *Katz* outlined a two-pronged test for evaluating whether government conduct violates an individual's reasonable expectation of privacy, thus constituting an illegal search.[48]

---

communication facility for the transmission . . . of bets or wagers on any sporting event or contest. . . ." 18 U.S.C. § 1084 (1994).

43. *Katz*, 389 U.S. at 348.

44. *Id.* at 351 ("[W]hat he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

45. *Id.* at 352.

46. *Id.* at 353.

47. The reasonable expectation of privacy standard was followed in later cases. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 177 (1984) (stating that "the touchstone of Amendment analysis has been the question whether a person has a 'constitutionally protected reasonable expectation of privacy'"); Smith v. Maryland, 442 U.S. 735, 740 (1979) (noting that the United States Supreme Court has uniformly held that application of the Fourth Amendment depends on whether the person invoking its protection can claim a "justifiable," "reasonable," or "legitimate expectation of privacy"); United States v. White, 401 U.S. 745, 752 (1971) (discussing what "constitutionally justifiable" means in terms of Fourth Amendment protection).

48. *Katz*, 389 U.S. at 361 (Harlan, J., concurring). *But see* HALL, *supra* note 18, at 51 (explaining that because the Supreme Court was trying to move away from using a specific formula for solving all Fourth Amendment problems, the opinion cannot be read as trying to adopt a new formula) (quoting Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 385 (1974)).

The majority never actually used the phrase "reasonable expectation of privacy." *See* HALL, *supra* note 18 at 51. However, the Supreme Court relies on this analysis, articulated by Justice Harlan, to determine if an individual has an expectation of privacy. *Id.* at 53. See *infra* notes 56-57 for examples of Supreme Court cases relying on the two-prong approach articulated by Justice Harlan.

First, an individual must demonstrate a subjective expectation of privacy.[49] Second, this expectation of privacy must be one which society is prepared to consider reasonable.[50]

1. Subjective Expectation of Privacy

If an individual cannot meet the threshold requirement of showing a reasonable expectation of privacy, then no search occurred, and the Fourth Amendment does not apply.[51] Whether an individual held a subjective expectation of privacy is evaluated by considering the precautions taken to preserve privacy.[52] For example, information voluntarily turned over to third parties[53] or placed in plain view[54] of the public indicates no intent to preserve privacy, and it affords no Fourth Amendment protection.[55] Precautions such as making a phone call from an enclosed telephone booth, however, indicate the caller's intent to keep the conversation private, even though the caller uses a public phone booth and is visible to the public.[56]

---

49. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

50. *Id.* (Harlan, J., concurring). Justice Harlan outlined the test as the following:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

Id. (Harlan, J., concurring).

51. Smith, 442 U.S. 735, 745-46 (1979).

52. *Katz*, 389 U.S. at 351. The majority in *Katz* expressed this element as follows: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* (citations omitted).

53. United States v. Jacobsen, 466 U.S. 109, 117 (1984) (explaining that when individuals expose private information to another party, the individuals have voluntarily undertaken a risk that the other party may reveal the information to government agents).

54. Oliver v. United States, 466 U.S. 170, 179 (1984).

55. *Id.*

56. *Katz*, 389 U.S. at 353; *see also* HALL, *supra* note 18, at 57. However, the phone numbers dialed from the phone booth lack a reasonable expectation of privacy. Smith v. Maryland, 442 U.S. 735, 743 (1979). In *Smith*, the Supreme Court held the Government's use of a "pen register" to record the numbers made from a telephone did not violate the caller's reasonable expectation of privacy. *Id.* at 742. The caller voluntarily turned over these phone numbers to a third party, the telephone company, when placing the calls. *Id.* at 742-43. The court concluded that individuals maintain no

2. Objective Expectation of Privacy

Although courts consider an individual's subjective expectation of privacy, the controlling issue is whether or not society is prepared to accept this expectation as legitimate.[57] The factors that courts have considered to determine an objective expectation of privacy include property interests,[58] the use ascribed to the area searched, society's longstanding beliefs, current circumstances,[59] and legislative enactments.[60] For instance, society fails to recognize an expectation of privacy in oral conversations spoken in a public room[61] or for drugs

---

reasonable expectation of privacy in information they voluntarily forward to third parties. *Id.* at 743-44 (citations omitted).

57. In *United States v. Smith*, the court stated that "a subjective expectation of privacy does not, by itself, give rise to Fourth Amendment protection." United States v. Smith, 978 F.2d 171, 177 (5th Cir. 1992), *cert. denied*, 507 U.S. 999 (1993). "The expectation of privacy must be one that society is prepared to recognize as reasonable." *Id.* Additionally, the Supreme Court and other courts often phrase the threshold requirement of a "search" to exclude a subjective expectation of privacy in favor of society's expectation of privacy. *See, e.g., Oliver*, 466 U.S. at 182-83 ("[T]he correct inquiry is whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment."); *Jacobsen*, 466 U.S. at 113 ("A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed.").

The Supreme Court noted that evaluating a subjective expectation of privacy may not adequately protect individuals' Fourth Amendment rights. Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979). In *Smith*, the Court explained that:

> Situations can be imagined, of course, in which Katz' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects.

Id. See HALL, *supra* note 18, at 54-55 for further commentary on excluding the subjective expectation of privacy from "search" analysis.

58. Rakas v. Illinois, 439 U.S. 128, 143-44 n.12 (1978). Courts derive society's reasonable expectations of privacy "by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Id. But see* Michael Campbell, *Defining a Fourth Amendment Search: A Critique of the Supreme Court's Post-Katz Jurisprudence*, 61 WASH. L. REV. 191 (1986) (criticizing the Berger Court for using arbitrary and inconsistent criteria to determine which searches were reasonable); Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583 (1989) (arguing post-*Katz* interpretations deviate from the principles espoused in *Katz* and tilt the balance in the government's favor).

59. The *Katz* court recognized the importance now placed on the public telephone in the realm of private communications. *Katz*, 389 U.S. at 352.

60. *See infra* Part II.C.2 (discussing the Electronic Communications Privacy Act of 1986).

61. *In re* John Doe Trader Number One, 894 F.2d 240, 245 (7th Cir. 1990) (holding that the trader's statements made on floor of mercantile exchange lacked a reasonable expectation of privacy).

grown in an open field.[62]

Once a court finds that an individual possesses a reasonable expectation of privacy, government actions are scrutinized to ensure that law enforcement officials conducted a search within constitutional limitations.[63] If, however, a court finds the individual lacked a reasonable expectation of privacy, the degree of intrusiveness of government actions is irrelevant because no constitutionally protected search occurred.[64]

C. Congressional Responses

Although the *Katz* Court determined the wiretapping in that case to be illegal, the Court recognized that a wiretap could have legally transpired if the government had followed procedures to safeguard against unnecessary invasions of privacy.[65] In *Berger v. New York*,[66] the Supreme Court actually articulated standards for government wiretapping based on the standards of a constitutional search and seizure.[67] Taking its cue from the Supreme Court, Congress aligned with modern technology by codifying the principles of *Berger* and *Katz* in Title III of the Omnibus Crime and Safe Streets Act of 1968 ("Title III").[68] Both Title III and subsequent legislation represent Congressional efforts to balance the government's need to use the latest technology as a tool to fight organized crime,[69] while at the same

62. Oliver v. United States, 466 U.S. 170, 179 (1984) (holding that open fields are not a setting for the intimate activities the Fourth Amendment is intended to protect).

63. *See Jacobsen*, 466 U.S. at 114 (stating that warrantless searches of sealed packages violate the Fourth Amendment since owners hold a reasonable expectation of privacy). In Berger v. New York, 388 U.S. 41 (1967), the Supreme Court articulated standards for wiretapping once a reasonable expectation of privacy is found. *Id.*, at 58-60. The Court stated that the following constitutional standards are required before the issuance of a wiretap: (1) A showing of probable cause for the initial warrant and for a continuance; (2) particularity in describing the place to be searched and the type of conversation sought; (3) a specified termination date of the eavesdrop once the information is seized; (4) a showing of an emergency situation to overcome proper notice requirements; and (5) a return by the government showing what was seized under the warrant. *Id.*

64. *See Smith*, 442 U.S. at 740 (stating that the Fourth Amendment only applies upon a violation of an individual's reasonable expectation of privacy).

65. *Katz*, 389 U.S. at 354 (1967) (failing to obtain proper authorization from a magistrate prior to the wiretap made search illegal).

66. 388 U.S. 41 (1967).

67. See *supra*, note 63, for the standards set out by the *Berger* court.

68. S. REP. NO. 1097, 90th Cong., 2d Sess. 76 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2163. A current version of the statute may be found at 18 U.S.C.A §§ 2510-2522 (West 1978 & Supp. 1996).

69. The section of the Senate Report regarding Title III emphasizes that "[t]he major purpose of Title III is to combat organized crime." S. REP. NO. 1097, 90th Cong., 2d

time addressing the risks to individual privacy created by this technology.[70]

1. Title III of the Omnibus Crime and Safe Streets Act of 1968

Title III codifies Fourth Amendment principles as applied to oral and wire communications.[71] It generally proscribes the interception or

---

Sess. 70 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2157. The insulation of top members in crime circles, and the unwillingness of fearful or apathetic witnesses to testify, leaves wiretapping as the most effective method to learn of criminal activities. *Id.* at 2159. See *infra* notes 71-85 for a discussion of Title III.

70. S. REP. NO. 1097, 90th Cong., 2d Sess. 66 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2122, 2153; *see also* S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559 (enacting legislation that amended the 1968 Act and explaining that the legislation represents a "fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies"); H.R. REP. NO. 827, 103d Cong., 2d Sess. 13 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3493 (explaining that the Digital Telephony Act of 1994 seeks to preserve a balance among the need for law enforcement to conduct investigations, individuals' privacy rights in light of emerging communication technologies, and the development of new technologies).

71. Title III of the 1968 Act defined oral communication as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." 18 U.S.C. § 2510(2) (Supp. IV 1968) (amended 1986). The 1968 Act was amended in 1986 by the Electronic Communications Privacy Act of 1986, ["ECPA"] Pub. L. No. 99-508, § 101(a)(2). *See* 18 U.S.C. § 2510(2) (1994). The definition of oral communication under the ECPA is "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.*" *Id.* § 2510(2) (emphasis added).

Title III of the 1968 Act defined wire communication as:

> [A]ny 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.

18 U.S.C. § 2510(1) (Supp. VI 1968) (amended 1986). The 1968 Act was amended by the ECPA, Pub. L. No. 99-508, § 101(a)(1). 18 U.S.C. § 2510(1) (1994). Under the ECPA, wire communication is defined as:

> [A]ny *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)* 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 *or communications affecting interstate commerce and such term includes any electronic storage of such communication.*

Id. § 2510(1) (emphasis added). See *infra* text accompanying notes 86-103 for a discussion of the 1986 amendments to Title III of the Omnibus Crime and Safe Streets Act of 1968.

disclosure of such communications,[72] while making provision for law enforcement to intercept these communications for use in criminal investigations.[73] An unauthorized "interception"[74] of protected

72. 18 U.S.C. § 2511(1) (Supp. IV 1968) (amended 1986). "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 . . . shall be fined not more than $10,000 or imprisoned not more than five years, or both." *Id.* The 1968 statute was amended by the ECPA, Pub. L. No. 99-508, § 101(c)(1)(A) (adding "electronic communications" to the type of communications protected under the Act), § 101(d)(1) (modifying the punishment) and § 101(f) (substituting "intentionally" for "willfully"). 18 U.S.C. § 2511(1) (1994).

73. *See* 18 U.S.C. § 2516 (Supp. IV 1968) (amended 1986) (explaining generally the procedures for authorizing interception of protected comunications). Only the Attorney General, or any specially designated Deputy Assistant Attorney General in the Criminal Division may authorize an application for the interception of wire or oral communications to a federal judge. *Id.* at § 2516(1). The 1968 Act was amended in 1986 by the ECPA, Pub. L. No. 99-508 to also include "any Assistant Attorney General." 18 U.S.C. § 2516(1) (1994), *amended by* AntiTerrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, § 434.

The interception carried out by the FBI or the Federal Agency responsible for the investigation may provide evidence of offenses related to specific crimes including, amongst others, racketeering, bribery of officials, murder, kidnapping, and fraud. 18 U.S.C. § 2516(1)(a-o) (Supp. IV 1968) (amended 1986). The AntiTerrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, § 434, modified § 2516(1)(n-p) to expand the authority of the Attorney General to also intercept communications related to the crime of alien smuggling. 18 U.S.C. § 2516(1)(n-p) (1994), *amended by* AntiTerrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, § 434.

A judge can grant an order to intercept communications if the judge finds that: (a) probable cause exists that an enumerated crime is happening or about to happen; (b) incriminating communications regarding that crime will be obtained by the interception; (c) normal investigative techniques will not work; and (d) the target of the interception is being used for a crime. 18 U.S.C. § 2518(3)(a-d) (Supp. IV 1968) (amended 1986) (1986 amendment substituted "wire, oral or electronic communication" for "wire or oral communication"). In addition, court orders must specify: (a) the identity of the person whose communications will be intercepted; (b) the place where the interception will occur; (c) a description of the type of communication sought, and to what crime it relates; (d) the identity of the agent authorizing the application; and (e) the time period for the interception. 18 U.S.C. § 2518(4)(a-e).

Interceptions are to continue only as long as necessary to obtain the sought communications and may not exceed thirty days. *Id.* at § 2518(5). Extensions may be granted under specified circumstances. *Id.*

After an interception, an inventory is turned over to the parties named in the order and to other parties of intercepted communications. 18 U.S.C. § 2518(8)(d) (Supp. IV 1968) (amended 1986). The inventory must include notice of (1) the fact of the order; (2) the date of the entry and period of authorization; (3) the fact that communications were or were not intercepted. *Id.* at § 2518 (8)(d)(1-3). The judge has discretion to reveal the intercepted communications to the parties. *Id.*

74. "'[I]ntercept' means the aural or other acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (Supp. IV 1968), *amended by* Electronic Communications Protection Act of 1986, Pub. L. No. 99-508, § 101(a)(4) (substituting "wire, oral, or electronic

communications is the government conduct that can result in an unconstitutional search.[75] Any unlawful interception or disclosure of oral or wire communications subjects the offender to civil damages[76] and can result in the suppression of the illegally obtained "fruits."[77]

Congress addressed the reasonable expectation of privacy requirements among its definitions of protected communications.[78] For instance, section 2510(2) of Title III only protects oral communications which are "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[79] This definition codifies the common law subjective and objective prongs of the reasonable expectation of privacy requirements.[80] An individual

---

communicaton" for "wire or oral communication").

75. 18 U.S.C. § 2511 (Supp. IV 1968) (amended 1986). The ambiguities involved with determining when more advanced communication technologies are intercepted are demonstrated in Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994). In this case, the Secret Service seized a computer used to operate an electronic bulletin board, which also held unread electronic mail messages of subscribers. *Id.* at 458. The subscribers argued the Secret Service "intercepted" their electronic mail communications because the messages had been sent but not yet received, "just as if someone had picked up and carried off a U.S. Postal Service mailbox from the side of the street." J. David Loudy, *Computer Seizures Implicate Numerous Laws*, CHI. DAILY L. BULL., July 13, 1995, at 6. The court, however, held an "interception" did not occur because the messages were seized while in electronic storage, not during transmission. *Steve Jackson Games, Inc.*, 36 F.3d at 461-62.

76. 18 U.S.C. § 2520 (Supp. IV 1968) (amended 1986).

77. 18 U.S.C. § 2518(10)(a) (1994). This section provides that:

> Any aggrieved person . . . before any court . . . may move to suppress the contents of any intercepted wire or oral communication, or evidence derived therefrom, on the grounds that—(i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval.

Id. This provision codifies the common-law "exclusionary rule" discussed *supra*, notes 15-18 and accompanying text.

78. *See* S. REP. NO. 1097, 90th Cong., 2d Sess. 75 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2162.

79. 18 U.S.C. § 2510(2) (Supp. IV 1968) (amended 1986). *See supra* note 71 (discussing the 1986 amendment).

80. *In re* John Doe Trader Number One, 894 F.2d 240, 242 (7th Cir. 1990) ("[T]his definition was intended to parallel the reasonable expectation of privacy test") (internal quotations omitted). *See also* Walker v. Darby, 911 F.2d 1573, 1578 (11th Cir. 1990) (stating that section 2510 requires the court to determine whether the party had a subjective expectation that conversations were free from interception and whether that expectation was objectively reasonable); *see also* Wesley v. WISN Division - Hearst Corp., 806 F. Supp. 812, 814 (E.D. Wis. 1992) ("The inquiry into whether one can reasonably expect to make communications free from interception is analogous to the inquiry into whether one has a reasonable expectation of privacy, as that term is used in the Fourth Amendment [search and seizure] context.").

pursuing a claim for illegally intercepting an oral conversation must show that: (1) under the subjective prong they did not suspect their conversation to be subject to interception;[81] and (2) under the objective prong, that expectation was justified by the circumstances.[82] Although neither Title III nor its legislative history indicate the circumstances under which an individual's expectation of privacy is justified, normal societal expectations govern.[83]

"Wire communication", however, is distinguished from "oral communication" because wire communication is defined without any expectation of privacy in its language.[84] A wire interception can violate Title III regardless of the communicator's expectation of privacy.[85]

2. Electronic Communications Privacy Act of 1986

For almost twenty years after its enactment, Title III remained the only codified protection against invasions of privacy for oral and wire communications.[86] With the advent of cellular telephones, computer-to-computer transmissions, and electronic mail systems, technology outpaced Title III statutory protections, leaving the existing law "hopelessly out of date."[87] When Senator Leahy, Chairman of the Senate Judiciary Subcommittee on Technology and the Law, asked the Attorney General whether interceptions of electronic mail were covered by Title III, the Justice Department responded that federal law protects electronic communications where a reasonable expectation of privacy

81. *Wesley*, 806 F. Supp. at 812. *But see In re* John Doe Trader Number One, 894 F.2d at 243 (broadening the subjective prong inquiry to whether the claimant generally held a subjective expectation of privacy instead of whether the claimant held an expectation that his conversation was free from possible interception).

82. Walker v. Darby, 911 F.2d 1573, 1578 (11th Cir. 1990) (explaining that a postal worker would need to show he held a subjective expectation that his conversations at his work place would be free from interception, and that this expectation was justified under the circumstances).

83. JAMES G. CARR, THE LAW OF ELECTRONIC SURVEILLANCE § 8.1(a)(3) (2d ed. Supp. 1995). *See also supra* note 50.

84. See *supra* note 71 for a definition of wire communication.

85. CARR, *supra* note 83, at § 8.1(a)(3). *See, e.g.*, Forsyth v. Barr, 19 F.3d 1527, 1535 n.14 (5th Cir. 1994) (quoting Briggs v. American Air Filter Co., Inc., 630 F.2d 414, 417 n.4 (5th Cir. 1980)), *cert. denied*, 115 S. Ct. 195 (1994); PBA Local No. 38 v. Woodbridge Police Dep't, 832 F. Supp. 808, 819 (D.N.J. 1993) (explaining that wire communications are protected regardless of any privacy expectations).

86. S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555.

87. *Id.* at 3556 (quoting 132 CONG. REC. S7992 (daily ed. June 19, 1986) (statement of Sen. Leahy)).

exists.[88] The Justice Department, however, admitted that with the newest technologies it is not always clear whether or not a reasonable expectation of privacy exists.[89] In an effort to update the existing law and keep pace with changing technology,[90] Congress enacted the Electronic Communications Privacy Act of 1986 ("ECPA") to amend Title III.[91] The ECPA consists of two parts: Title I and Title II.

Title I of the ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 by making the unauthorized interception of electronic communications illegal.[92] Congress also updated the existing act by adding "electronic" communications[93] to the type of communications which could be legally intercepted in criminal investigations.[94] "Oral communication," however, remains the only type of communication that explicitly requires an expectation of privacy.[95]

Codifying Fourth Amendment principles, Title I of the ECPA

88. S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557-58. *See also* Organizacion JD LTDA. v. United States Dep't of Justice, No. CV-92-3690, 1996 U.S. Dist. LEXIS 4347, at *8-*9 (E.D.N.Y. Apr. 2, 1996) (describing the impetus of the ECPA).

89. S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3558. The Justice Department stated that "[i]n this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as [whether there does or does not exist a reasonable expectation of privacy] are not always clear or obvious." *Id.*

90. H.R. REP. NO. 647, 99th Cong., 2d Sess. 18 (1986). "[D]espite efforts by both Congress and the courts, legal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology." *Id.*

91. Pub. L. No. 99-508, 100 Stat. 1848 (1986).

92. 18 U.S.C. § 2511 (1994).

93. The statute defines electronic communications as:

> [A]ny 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 photo-optical system that affects interstate or foreign commerce, but does not include - (A) any wire or oral communication; (B) any communication made through a tone-only paging device; or (C) any communication from a tracking device . . . .

18 U.S.C. § 2510(12) (1994), *amended by* AntiTerrorism Act and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, § 73 (adding subsection (D) to the definition of electronic communications, which provides: "(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds").

94. For an analysis of the other amendments made under Title I of the ECPA, see the Section-By-Section Analysis in S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3565-89.

95. *Compare* 18 U.S.C. § 2510(2) (1994) (defining oral communication) *with* 18 U.S.C. § 2510(1) (1994) (defining wire communication) *and* 18 U.S.C. § 2510(12) (1994) (defining electronic communication).

includes a provision emulating the plain view doctrine.[96] Protected communications that are revealed to the public lose their privacy expectations and therefore lose ECPA protection.[97] For example, a university may provide electronic mail service for use by its students. Electronic mail transmissions are protected electronic communications under the ECPA.[98] When a student transmits a message to another student, and the recipient must use a password to access their mail, the transmitting student holds a reasonable expectation of privacy in the transmission.[99] However, if the university sends an electronic mail message to all students, the university lacks any expectation of privacy in the transmissions and thus lacks ECPA protection.[100]

Title II of the ECPA makes illegal the unauthorized access to stored wire and electronic communications.[101] Under Title II, government agents authorized to access stored communications must retrieve the information from the service providers.[102] Title II specifically

---

96. 18 U.S.C. § 2511(2)(g)(i-ii) (1994). Part (i) of this section states that it is lawful "to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." *Id.* § 2511(2)(g)(i). Section 2511(2)(g)(ii) is a similar provision, but applies instead to radio communications.

97. *See* 18 U.S.C. § 2511(2)(g)(i) (1994).

98. 18 U.S.C. § 2510 (12) (1994) (defining electronic communication), *amended by* AntiTerrorism Act and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, § 731 (1996). *See also* S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568 ("This term [electronic communication] also includes electronic mail").

99. *See* United States v. Maxwell, 42 M.J. 568, 576 (C.M.A. 1995) (holding that recipient or sender of electronic mail maintains a reasonable expectation of privacy in transmissions which can only be accessed with a password), *reh'g granted in part*, 44 M.J. 41 (1996). *But see* Smyth v. Pillsbury, 914 F. Supp. 97 (E.D. Pa. 1996) (holding that an employee lacked a reasonable expectation of privacy in electronic communications sent to his supervisor over the intra-company electronic mail system).

100. *See Maxwell*, 42 M.J. at 576 (finding that privacy expectations disappear when electronic mail messages are downloaded by other subscribers). The ECPA, however, fails to mention any privacy expectations. *See* 18 U.S.C. § 2510(12).

101. 18 U.S.C. §§ 2701-2711 (1994). Section 2701(a) provides that:

> [W]hoever —(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 . . . .

18 U.S.C. § 2701(a).

102. 18 U.S.C. § 2703 (1994). This section outlines the requirements for government access as follows:

> 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 system for one

addresses computerized recordkeeping systems that store information for businesses, physicians, hospitals, and providers of electronic mail.[103]

3. Digital Telephony Act of 1994

More recently, Congress enacted the Communications Assistance for Law Enforcement Act of 1994 ("Digital Telephony Act")[104] "to preserve the government's ability . . . to intercept communications involving advanced technologies . . . while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services."[105] This Act requires telecommunication carriers, by 1998, to design systems to isolate and intercept communications requested by the government under court order.[106] Unlike the ECPA, Congress intended this Act to only facilitate government interceptions and clearly define the role of the telecommunication carriers in the process.[107] It does not address any privacy expectations of the telecommunication carriers' subscribers.[108]

III. DISCUSSION

When applying both the ECPA and the Fourth Amendment, courts must invariably address an individual's reasonable expectation of privacy.[109] The impact of the court's method of analysis turns on

---

hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant.

Id. at § 2703(a).

103. 18 U.S.C. § 2703. This section is in part a response to United States v. Miller, 425 U.S. 435 (1976), which held a bank customer lacked standing to contest disclosure of his bank records since he voluntarily turned them over to a third person. *Id.*

104. 47 U.S.C. §§ 1001-1010 (1994).

105. H.R. REP. NO. 827, 103rd Cong., 2d Sess. 9 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489. For a discussion of suggested political motivations behind the Act, see Rogier van Bakel, *How Good People Helped Make a Bad Law*, WIRED, Feb. 1996, at 133.

106. 47 U.S.C. §§ 1002(a), 1003(b) (1994). For a discussion of privacy expectations and the Digital Telephony Act, see Timothy B. Lennon, *Comment: The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 be like 1984?*, 58 ALB. L. REV. 467 (1994); Jim Warren, *Surveillance-on-Demand*, WIRED, Feb. 1996, 72 (criticizing the unnecessary intrusiveness of the Act).

107. As a result, the problem identifying whether an "interception" occurred as in *Steve Jackson Games, Inc.* is moot. *See supra* note 75. An "interception" will occur at the point of connection with the telecommunications carrier, not after electronic mail is sent but before it is retrieved.

108. *Compare* 47 U.S.C. § 1001 *with* 18 U.S.C. § 2510. Unlike the ECPA, none of the key terms defined in the Digital Telephony Act includes a reasonable expectation of privacy. 47 U.S.C. § 1001-1010.

109. Although communications technology may be protected by the ECPA, some

whether the communication is defined as oral, wire, or electronic. This classification determines the level of protection provided by the ECPA in comparison to the level of protection provided by the Fourth Amendment.[110] For example, evidence obtained illegally from electronic communications, unlike evidence obtained illegally from wire or oral communications, is not suppressed under the ECPA.[111] Thus, the only means for suppressing an electronic communication at trial is by showing a violation of the Fourth Amendment.[112] To prevail at showing a violation of the Fourth Amendment, the communicator must show the existence of a reasonable expectation of privacy. Like "wire communication," however, "electronic communication" is not defined with any privacy expectation necessary on behalf of the communicator.[113]

A court must then decide what role, if any, the inclusion or exclusion of an electronic communication technology from the ECPA plays in determining whether the communicator held a reasonable expectation of privacy. One approach courts take is to treat the

---

courts may never even mention the ECPA when rendering a decision. *See, e.g.*, United States v. Chan, 830 F. Supp. 531 (N.D. Cal. 1993). In *Chan*, government agents seized and retrieved information from a pager. *Id.* at 533. Although pagers are considered an "electronic communication" under the ECPA, the court only evaluated Chan's reasonable expectation of privacy in the pager to determine that no search occurred. *Id.* at 534.

110. On its face, the ECPA provides the same level of protection to oral communications as does the Fourth Amendment. *See* 18 U.S.C. § 2510(2). In accordance with the ECPA and the Fourth Amendment, a court can suppress evidence illegally obtained from an oral communication if the communicator held a reasonable expectation of privacy. *See id.; see also* 18 U.S.C. § 2515 (1994) (prohibiting the use of evidence obtained from an illegally intercepted oral communication).

Wire communications are afforded greater protection under the ECPA than under the Fourth Amendment. *See* 18 U.S.C. § 2510(1) (1994). Whereas evidence obtained from a wire communication may only be suppressed upon a finding that the communicator held a reasonable expectation of privacy, no such finding is required under the ECPA. Forsyth v. Barr, 19 F.3d 1527, 1534 n.14 (5th Cir.), *cert. denied*, 115 S. Ct. 195 (1994); *see also* 18 U.S.C. § 2510(1) (defining wire communication without any privacy expectations). To suppress evidence from a wire communication under the ECPA, a court need only find that the illegal "interception" of a "wire communication" occurred. *See* 18 U.S.C. § 2515. Unlike the definition of "oral communication," "wire communication" is not defined with any privacy expectations on behalf of the communicator. *Id.*

111. *See* 18 U.S.C. § 2515 (suppressing only evidence from wire and oral communications). Only a civil remedy is available to the victim of an illegal electronic communication interception. *See* 18 U.S.C. § 2520 (1994).

112. *See* United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990) (holding that unless a violation of Meriwether's Fourth Amendment rights is shown, the intercepted electronic communication cannot be suppressed).

113. See *supra* notes 71 and 93 for the definitions of "wire" and "electronic" communication, respectively. See *supra* note 71 and accompanying text for the contrasting definition of "oral" communication.

inclusion or exclusion of a communication technology from the ECPA as irrelevant for a Fourth Amendment analysis.[114] Another approach is to hold that the inclusion of a communication technology in the ECPA supports the legitimacy of the communicator's expectation of privacy.[115]

A. Inclusion or Exclusion from the ECPA Irrelevant to Fourth Amendment Analysis

In *United States v. Meriwether*,[116] the Sixth Circuit applied a separate Fourth Amendment analysis, independent of an ECPA analysis, to determine whether to suppress evidence obtained from a digital display-type pager.[117] Pagers satisfy the definition of an electronic communication under the ECPA.[118] Therefore, under the ECPA, communications made via pagers are protected from unwarranted interceptions, although such evidence is not suppressible in a criminal trial.[119]

In *Meriwether*, drug enforcement agents seized a digital display pager under a search warrant which authorized them to seize "'all evidence of narcotics and controlled substance use . . . including address books, notebooks, cash, records, papers, ledgers, tallysheets, [and] telephone numbers of customers, suppliers, [and] couriers.'"[120] Agents recorded the phone numbers coming in to the pager, including that of the defendant.[121] Chosen at random from incoming phone numbers, agents called the defendant's number, arranged to purchase cocaine from the defendant, and ultimately arrested him.[122]

---

114. *See infra* Part III.A.

115. *See infra* Part III.B.

116. 917 F.2d 955 (6th Cir. 1990).

117. *Id.* at 958-59.

118. *See id.* at 959-60; *see also* 18 U.S.C. § 2510(12) (1994) (defining electronic communications), *amended by* AntiTerrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, § 73 (expanding definition of electronic communication). See *supra* note 93 for discussion of recent amendment.

This type of pager is distinguished from a tone-only paging device which is specifically excluded under the definition of 'electronic communication.' 18 U.S.C. § 2510(12)(B).

119. 18 U.S.C. § 2511 (1994).

120. *Meriwether*, 917 F.2d at 957.

121. *Id.*

122. *Id.*

Meriwether moved to suppress evidence at trial based on a violation of his Fourth Amendment rights[123] and a violation under the ECPA.[124] The court provided distinct, independent analyses for each of these arguments.[125] The court first considered whether or not an unreasonable search of Meriwether's phone number, which would be protected by the Fourth Amendment, occurred.[126] The court evaluated Meriwether's reasonable expectation of privacy argument without any reference to the inclusion of pagers as protected electronic communications within the ECPA.[127] Instead, the court followed the *Katz* two-prong analysis of whether an individual exhibited a subjective expectation of privacy and whether that expectation is objectively reasonable by society's standards.[128]

Under the first prong, the court reasoned that Meriwether lacked even a subjective expectation of privacy because he transmitted information to a device over which he had no control.[129] The court compared transmitting information to a pager with transmitting information by making a telephone call.[130] Whereas a caller risks making incriminating statements to the wrong person over the telephone, a person sending a message to a pager increases that risk by transmitting data without any immediate feedback by the recipient.[131] Thus the sender voluntarily undertakes the risk that someone else might be in possession of the pager.[132] The court reasoned that circumstances showing that Meriwether disregarded the possibilities of unintended recipients of his transmission indicated that he lacked a subjective expectation of privacy.[133]

---

123. Part of Meriwether's Fourth Amendment argument was that the seizure of his phone number from the pager was beyond the scope of the search warrant. *Id.* at 958. The court dismissed this contention, reasoning that a warrant authorizing the search for telephone numbers of customers included a telephone pager, which "by its very nature, is nothing more than a contemporary receptacle for telephone numbers." *Id.*

124. Meriwether argued the search of the pager constituted an illegal "interception" under Title III as revised by the ECPA. *Id.* at 959. Under the ECPA, however, evidence intercepted from electronic communications may not be suppressed at trial. *See* 18 U.S.C. § 2515 (1994) (prohibiting evidence intercepted from only oral or wire communications). Thus, a successful argument under the ECPA would not have helped Meriwether.

125. *Meriwether*, 917 F.2d at 958-960.

126. *Id.* at 958.

127. *Id.* at 958-59.

128. *Id. See supra* Part II.B. (discussing two-prong analysis in *Katz*).

129. *Meriwether*, 917 F.2d at 959.

130. *Id.*

131. *Id.*

132. *Id.*

133. *Id.*

Once Meriwether failed the subjective prong of the *Katz* two-prong analysis, the court found no need to evaluate Meriwether's privacy expectations under the objective prong of the test.[134] The court ignored the fact that the ECPA protected pager communications when deciding whether to suppress this evidence. The court instead focused solely on the Fourth Amendment analysis. Under the Fourth Amendment analysis, the court found that no reasonable expectation of privacy existed and held that Meriwether was not subjected to a search.[135]

The court then began a new analysis that addressed whether obtaining Meriwether's phone number from the pager constituted an interception under section 2511 of the ECPA.[136] In holding that pagers are generally covered by the ECPA, the court relied on the legislative history explicitly proscribing the unauthorized interception of data transmissions to display pagers transmitted by a common carrier.[137] The legislative history did not explicitly state that pagers receive statutory protection because a person transmitting data to a pager maintains a legitimate expectation of privacy.[138] The Senate Report quoted by the court did, however, imply that pager communications should receive protection because individuals use pagers with a reasonable expectation of privacy, since pagers are "not readily accessible to the general public."[139] Nevertheless, the court chose not to interpret this language as granting a reasonable expectation of privacy to communications transmitted via pagers for purposes of a Fourth Amendment analysis.[140]

The legislative history, as interpreted by the court, meant that only those communications in the process of being transmitted to a pager were protected against unauthorized interception.[141] In other words, an interception could only occur between the time a sender entered his

134. *Id.*

135. *Id.*

136. *Id.* at 959-60.

137. *Id.* at 960. "The unauthorized interception of a display paging system, which includes the transmission of alphanumeric characters over the radio, carried by common carrier, is illegal." *Id.* (quoting S. REP. NO. 541, 99th Cong. 2d Sess. 15 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3569).

138. *Id.* (quoting S. REP. NO. 541, 99th Cong. 2d Sess. 15 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3569).

139. *Id.* (quoting S. REP. NO. 541, 99th Cong. 2d Sess. 15 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3569).

140. *Meriwether*, 917 F.2d at 960.

141. *Id. See also* United States v. Reyes, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (concluding that an "interception" must occur simultaneously as a data transmission for ECPA purposes).

alphanumerical message and the pager emitted a signal that a transmission had been received.[142] In this case, the agents retrieved Meriwether's phone number after the transmission ended.[143] Although the ECPA protected against the unauthorized interception of pager communications, the court concluded that no interception occurred.[144]

Unlike *Meriwether* where the ECPA afforded protection to pagers, in *United States v. Smith*[145] the Fifth Circuit evaluated the privacy expectations of a defendant who used a communication technology specifically *excluded* from the ECPA.[146] In *Smith*, the Fifth Circuit considered a motion to suppress evidence intercepted from the defendant's cordless telephone.[147] The court evaluated this motion by proceeding under independent analyses for the ECPA and the Fourth Amendment without considering any privacy expectation implications based on the specific provision excluding cordless telephones from the ECPA.[148]

Based on precedent as well as the text and legislative history of the

142. The Fifth Circuit expressed a similar view of when an "interception" takes place with electronic communications in Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994). See *supra* note 75 discussing this issue in *Steve Jackson Games, Inc.*

143. *Meriwether*, 917 F.2d at 960.

144. *Id.* at 957. The court ignored a possible claim under Title II of the ECPA prohibiting the unauthorized access of stored electronic communications. *See* 18 U.S.C. § 2701 (1994). Since the transmission ended by the time the officers retrieved the phone number, the phone number was arguably stored in the limited memory of the pager. *Meriwether*, 917 F.2d at 957.

In a similar case, a federal district court did follow this line of reasoning and found a violation under Title II. United States of America v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996). In *Reyes*, government agents accessed stored numbers from a pager without authorization. *Id.* at 837. The court had to determine whether accessing the stored numbers constituted a violation under Title I or Title II. *Id.* at 837-38. Relying in part on the Sixth Circuit's holding in *Meriwether*, that accessing stored numbers from a pager is not an interception under Title I, the court consequently concluded the agents accessed stored communications in violation of Title II. *Id.* at 837. However, the court ignored the fact that section 2701 applies to the access of *facilities* where electronic communications are stored. See *supra* note 101 for the applicable text of section 2701(a). Furthermore, the legislative intent shows that Title II was intended to protect facilities such as a computer mail facility or a remote computing service, not an individual pager. *See* S. REP. NO. 541, 99th Cong., 2d Sess. 15 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3590.

The Digital Telephony Act of 1994 will help better determine when an "interception" occurs as the telecommunication carriers will provide technology to intercept communications. *See* 47 U.S.C. § 1002(a) (1994); *see supra* text accompanying notes 104-108 discussing the Digital Telephony Act.

145. 978 F.2d 171 (5th Cir. 1992).

146. *Id.* at 173, 175.

147. *Id.* at 173.

148. *Id.* at 174-81.

ECPA, the court first concluded that cordless phones are excluded from statutory protection.[149] The court pointed to the definitions of "wire communication"[150] and "electronic communication"[151] which explicitly excluded the radio component of a cordless phone communication occurring between the handset and the base of a cordless phone.[152] This radio portion of the communication is easily intercepted with an AM radio.[153] Congress therefore deemed it "inappropriate to make the interception of such a communication a criminal offense."[154] The definition of "oral communication"[155] also failed to protect the cordless phone conversation.[156] By limiting the definition to communications carried by sound waves only, Congress intended to exclude any communications carried by radio waves from inclusion in the definition of "oral communication".[157]

As the Fifth Circuit failed to find the cordless phone conversation an oral, wire, or electronic communication under the ECPA definitions, the court then analyzed whether an unreasonable search occurred under the Fourth Amendment.[158] To determine whether a search occurred,

149. *Id.* at 175-76. Communications over cordless phones are no longer excluded under the definitions of "wire communications" and "electronic communications." 18 U.S.C. § 2510(1), (12) (1994).

150. United States v. Smith, 978 F.2d 171, 175 n.2 (5th Cir. 1992). See *supra* note 71 for definition of "wire communication." Before the 1994 amendment, this definition included the language: "'wire communication' . . . does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit." 18 U.S.C. § 2510(1)(Supp. IV 1986) (amended 1994).

151. *Smith*, 978 F.2d at 175 n.4. *See supra* note 93 for the definition of "electronic communication." Before the 1994 amendment, this definition included the language: "'electronic communication' . . . does not include - (A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit." 18 U.S.C. § 2510(12) (Supp. IV 1986) (amended 1994).

152. *Smith*, 978 F.2d at 175 n.2, n.4. A cordless telephone is comprised of a handset into which the caller speaks, and a base unit wired to a landline. S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3563. A communication is transmitted by radio waves from the handset to the base unit, and from the base unit through the landwire. *Id.*

153. *Smith*, 978 F.2d at 179. *See also* S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566.

154. *Smith*, 978 F.2d at 176 (quoting S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566).

155. *Id.* at 175 n.3. See *supra* note 71 for the definition of "oral communication."

156. *Smith*, 978 F.2d at 176.

157. *Id.* at 175-76 (citing S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567).

158. *Smith*, 978 F.2d at 176-81.

the court examined whether the defendant's subjective expectation of privacy[159] was one that society considered "reasonable."[160]

Earlier analysis under the ECPA was irrelevant to the court's Fourth Amendment evaluation.[161] Despite the earlier ECPA analysis excluding cordless phones from statutory protection, the court explained that cordless phone users cannot be dismissed as lacking a reasonable expectation of privacy simply because they used a cordless phone.[162] Instead, the court considered the specific technology used and the surrounding circumstances to determine if the defendant's subjective expectation of privacy was reasonable.[163] Recognizing that the technology of cordless phones had evolved to decrease the ability to intercept transmitted radio waves,[164] the court acknowledged that this evolution increased the objective reasonableness of an expectation of privacy.[165] Although the Fifth Circuit was willing to evaluate whether the defendant maintained an expectation of privacy that society would consider reasonable, the court noted that Smith failed to offer evidence to prove that his subjective expectation of privacy was reasonable based on the technological advancements of his particular cordless phone.[166] Therefore, the court affirmed a denial of the defendant's motion to suppress evidence collected through monitoring his cordless phone calls.[167]

159. Smith contended he did not know his conversation could be easily intercepted. *Id.* at 177.

160. *Id.* at 177.

161. *Id.* at 176-81.

162. *Id.* at 180.

163. *Id. Contra* Oliver v. United States, 466 U.S. 170, 181 (1984). The Court argued that a case-by-case approach to determine whether particular circumstances justify a reasonable expectation of privacy would hinder police efforts to conduct searches because it would require subjective line drawing by agents prior to each search. *Oliver*, 466 U.S. at 181. The *Oliver* Court noted that: "The lawfulness of a search would turn on '[a] highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts and requiring the drawing of subtle nuances and hairline distinctions. . . .'" *Id.* (quoting New York v. Belton, 453 U.S. 454, 458 (1981) (quoting Wayne LaFave, *"Case-By-Case Adjudication" versus "Standardized Procedures": The Robinson Dilemma*, 1974 SUP. CT. REV. 127, 142)).

164. The technological advancements of cordless phones include multiple frequencies, frequencies not used by commercial radio, and encryption. *Smith*, 978 F.2d at 179.

165. *Id.*

166. *Id. But cf.* Askin v. McNulty, 47 F.3d 100 (4th Cir. 1995) (admitting reluctance to find Fourth Amendment protection for cordless phone users in contravention of the cordless phone exception in Title III), *cert. denied*, 116 S. Ct. 382 (1995).

167. *Smith*, 978 F.2d at 181.

B. Inclusion in the ECPA Relevant to Fourth Amendment Analysis

Unlike the courts in *Meriwether* and *Smith*, the United States Air Force Court of Criminal Appeals in *United States v. Maxwell*[168] alluded to the premise that the inclusion of a specific technology in the ECPA implied a reasonable expectation of privacy attached to the user of that communication.[169] In this case, Colonel Maxwell subscribed to and transmitted electronic mail messages through America Online, an internet network service provider.[170] Maxwell used five different screen names to transmit messages, and he thus had five separate "mailboxes" in which messages were stored and retrieved.[171] During an FBI investigation of child pornography transmitted through America Online networks,[172] one of Maxwell's screen names was identified for investigation.[173] In anticipation of a search warrant to seize communications of alleged perpetrators, America Online identified and extracted communications under *all* of Maxwell's screen names.[174] Thus, even those communications made under Maxwell's four other screen names, which were not under investigation, were turned over to the FBI.[175]

The trial court dismissed Maxwell from the Air Force based on this incident.[176] He appealed, contending that the seizure of information from the America Online computers violated his Fourth Amendment rights and should have been excluded at trial.[177] The court weighed Maxwell's reasonable expectation of privacy under traditional Fourth

168. 42 M.J. 568 (C.M.A. 1995).

169. *Id.* at 576.

170. *Id.* at 573.

171. *Id.* Subscribers use screen names to access the service so that other members can identify each other anonymously. *Id.* Individual subscribers can use up to five different screen names, but each screen name corresponds to only one person. *Id.*

172. A two year FBI investigation of child pornography distribution over America Online came to a climax with searches of over 120 homes nationwide, and at least a dozen arrests in September of 1995. Jared Sandberg, *U.S. Cracks Down on On-Line Child Pornography*, WALL ST. J., Sept. 14, 1995, at A3.

173. United States v. Maxwell, 42 M.J. 568, 574 (C.M.A. 1995).

174. *Id.*

175. *Id.*

176. *Id.* at 573.

177. *Id.* at 575. Maxwell also contested a search of his on-base quarters by military officials which resulted in seizure of incriminating images from his personal computer. *Id.* Maxwell claimed the warrant failed to describe with particularity which items were to be seized. *Id.* The court found, however, that the warrant was sufficient. *Id.* at 579.

Amendment doctrine and alluded to the ECPA as support for its findings.[178]

Contrary to the lower court's finding,[179] the Court of Criminal Appeals recognized that an objective expectation of privacy remained with the sender of electronic mail which remained stored on the America Online computers.[180] The use of passwords and screen names assured that only the intended recipients could retrieve the communications.[181] Thus, electronic mail subscribers actually held a higher level of objective privacy than individuals making telephone calls that could be answered by anyone.[182]

The court relied predominantly on a Fourth Amendment analysis to find society recognized this expectation of privacy.[183] The court stated that "[i]n the modern age of communications, society must recognize such expectations of privacy as reasonable."[184] Without any discussion or analysis under the ECPA, the court concluded that the ECPA supports society's recognition of this privacy expectation.[185] Once the court was satisfied that Maxwell held a reasonable expectation of privacy in his communications, the court refrained from further ECPA analysis such as whether government agents properly carried out the interception or properly accessed the stored communications.[186]

---

178. *Maxwell*, 42 M.J. at 576 (C.M.A. 1995).

179. The military judge found that while Maxwell held a subjective expectation of privacy, he lacked an objective expectation of privacy because, "(1) the e-mail could not be recalled or erased once it was dispatched . . . (2) the e-mail messages were transferred to screen names rather than to known individuals, and (3) the forwarding of messages to multiple individuals made the situation analogous to bulk mail. . . . [The] appellant was seeking anonymity rather than privacy. . . ." *Id.*

180. *Id.*

181. *Id.*

182. *Id.* *See supra* text accompanying notes 116-133 (sending a message to a pager has a lesser expectation of privacy than making a phone call).

183. *Maxwell*, 42 M.J. at 576.

184. *Id.*

185. *Id.* Although the court found that Maxwell maintained a reasonable expectation of privacy, probable cause still existed to search the communications seized under one of Maxwell's screen names. *Id.* at 577. Although no probable cause existed to search communications stored under Maxwell's other screen names, the court found a "good faith exception" existed to allow these incriminating communications to be admitted into evidence. *Id.* at 578. The communications made under Maxwell's other screen names were not requested by the FBI. *Id.* at 574. America Online collected them in anticipation of an FBI search warrant, and turned them over to the FBI upon receipt of the search warrant. *Id.* at 579.

186. The court could have evaluated this conduct under 18 U.S.C. §§ 2511 and 2701. *See* 18 U.S.C. § 2511 (1994) (prohibiting the interception of wire, oral or electronic communications); 18 U.S.C. § 2701 (1994) (defining unlawful access to stored

IV. ANALYSIS

With the exception of *Maxwell*, other courts have disregarded whether the inclusion or exclusion of a communication technology from the ECPA is relevant to determine the communicator's reasonable expectation of privacy.[187] However, based on the legislative history (relied on by the courts in *Meriwether* and *Smith*[188]) the inclusion or specific exclusion of a communication technology from the ECPA is probative of the objective reasonableness of the communicator's alleged privacy expectations. Therefore, the approach adopted by the court in *Maxwell*, which recognizes that the inclusion of a communication technology in the ECPA implies that the communicator held an objectively reasonable expectation of privacy, is the approach the *Meriwether* and *Smith* courts should have followed.[189]

A. Accessibility as Determining Factor to ECPA Inclusion

Both the *Meriwether* and *Smith* courts relied on excerpts from the legislative history of the ECPA to support denial of Fourth Amendment protection to the defendants in those cases.[190] The legislative history the courts relied upon, however, supported a finding that the question of whether a technology is included in the ECPA merits consideration when undertaking a traditional Fourth Amendment analysis. A review of the legislative history reveals that whether a communication technology is included in the ECPA turns on whether it is easily intercepted by (or accessible to) the general public.[191]

For instance, the *Meriwether* court quoted a portion of a Senate Report that stated that "[r]adio communications transmitted over a system provided by a common carrier are not readily accessible to the general public . . . ."[192] The rest of this sentence in the Senate Report names a tone-only paging system as an exception to radio

---

information).

187. *See, e.g.*, United States v. Smith, 978 F.2d 171, 176-77 (5th Cir. 1992) (cordless telephone); United States v. Meriwether, 917 F.2d 955, 958-959 (6th Cir. 1990) (digital display pager); United States v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996) (digital display pager).

188. *See supra* Part III.A.

189. *See infra* notes 190-216 and accompanying text.

190. *See supra* text accompanying notes 136-157.

191. *See, e.g.*, S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3569. "[T]he Electronic Communications Privacy Act provides an exception to the general prohibitions on interception for electronic communications which are configured to be readily accessible to the general public." *Id.*

192. *Meriwether*, 917 F.2d at 960.

communications not readily accessible to the general public.[193] Consequently, tone-only paging systems are not protected by the ECPA.[194] Nonetheless, citing to a Senate Report finding that the type of pager at issue in *Meriwether* was inaccessible to the general public played no role in the court's Fourth Amendment analysis.[195]

Similarly, the Fifth Circuit in *Smith* also relied on language of the Senate Report relating to the ease of accessibility of cordless phone communications.[196] The *Smith* court pointed to language explaining that the rationale for *excluding* cordless phones from statutory protection stemmed from their ease of interception.[197] The full sentence of the Senate Report, which is quoted in part by the *Smith* court, explains 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."[198] The ease of intercepting cordless phone communications at the time of the incident, however, failed to carry any weight in determining whether Smith held a reasonable expectation of privacy warranting exclusion under the Fourth Amendment.[199]

Using the accessibility of a particular communication technology as the criterion for its inclusion within the ECPA has garnered further support from Congress' reaction to advanced cordless phone technology.[200] In 1994, Congress amended the definitions of "wire communication" and "electronic communication" to include communications over cordless telephones.[201] As technological advancements increased the user's expectation of privacy in cordless

193. S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3569. *See also* 18 U.S.C. § 2510(12)(B) (1994) (explicitly excluding tone-only paging devices from statutory protection).

194. 18 U.S.C. § 2510(12)(B).

195. *See supra* notes 116-33 and accompanying text.

196. United States v. Smith, 978 F.2d 171, 176 (5th Cir. 1992).

197. *Id.* (quoting S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566).

198. S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566.

199. *See supra* text accompanying notes 145-67 and accompanying text.

200. *Smith*, 978 F.2d at 179. Advancements in cordless telephone technology include a limited broadcast range, multiple frequencies, and the use of noncommercial radio frequencies. *Id.*

201. *See* 18 U.S.C. § 2510(1), (2) (1994). For a discussion explaining why cordless telephones should be included under the ECPA, see Timothy R. Rabel, Comment, *The Electronic Communications and Privacy Act: Discriminatory Treatment for Similar Technology, Cutting the Cord of Privacy*, 23 J. MARSHALL L. REV. 661 (1990).

phones, Congress brought these communications under protection of the ECPA.[202]

Finally, the language of the statute itself supports this premise.[203] The provision, analogous to the common law plain view doctrine, indicates that electronic communications generally accessible by the general public are not protected.[204]

B. The Link between Accessibility, Inclusion within the ECPA, and Determining Whether a "Search" Occurred

Courts should consider the ease of intercepting a communication transmitted by a particular technology when determining whether the sender of the communication held an objectively reasonable expectation of privacy. As discussed above,[205] to satisfy the objective prong of the *Katz* two-prong analysis in determining whether a search occurred, the individual's expectation of privacy must be one that society is prepared to find legitimate.[206] If a communication technology is easily susceptible to interception, as in *Meriwether*, then this reduces the legitimacy of the communicator's claim to an expectation of privacy.[207] In other words, if the general public can easily access an individual's communication, then society is less likely to find it was reasonable for that particular individual to expect the communication to remain private.[208]

On the other hand, recognition of the difficulty in accessing a particular communication technology, as in *Maxwell*, supports the reasonableness of the communicator's alleged privacy expectations.[209] For instance, the *Maxwell* court found that the difficulty for the general public to access Colonel Maxwell's electronic mail messages sent to

202. *See* Pub. L. No. 103-414, § 202(a)(1-2) (striking the part of the definitions of wire and electronic communication which excluded the radio portion of a cordless telephone communication that is transmitted between the handset and the base unit).

203. *See* 18 U.S.C. § 2511(2)(g)(i) (1994).

204. See *supra* text accompanying notes 96-100 for discussion of the plain view doctrine as codified in the ECPA.

205. *See supra* Part II.B.

206. *See supra* notes 57-62 and accompanying text.

207. *See* United States v. Smith, 978 F.2d 171, 179 (5th Cir. 1992) (analyzing a comparable case in which the relative ease of overhearing a cordless phone conversation failed to warrant a reasonable expectation of privacy on behalf of the caller).

208. *See id.*

209. *See id.* The *Smith* court explained: "Surely the reasonableness of an expectation of privacy becomes greater when the [cordless telephone] conversation can only be intercepted using specialized equipment not possessed by the average citizen." *Id.*

other subscribers supported the objective reasonableness of Colonel Maxwell's claimed expectation of privacy.[210]

Once a court determines that communications are not readily accessible to the general public, and that the individual holds an objectively reasonable expectation of privacy, then the connection can be made between accessibility, inclusion or specific exclusion from the ECPA, and the reasonable expectation of privacy. If a wire or electronic communication technology is difficult to access by the general public, then it is probably protected by the ECPA.[211] Likewise, if the communication technology is difficult to access by the general public, then the communicator will probably hold a legitimate expectation of privacy.[212] Therefore, if a communication technology is protected by the ECPA, then the inclusion is probative of the legitimacy of the communicator's expectation of privacy and thus probative of whether a search occurred.

The *Maxwell* court came the closest to making this connection, albeit with little discussion.[213] Under the objective prong of the *Katz* two-prong analysis, the *Maxwell* court explained that Colonel Maxwell held a legitimate expectation of privacy in his electronic mail transmissions since he faced almost no risk of someone else intercepting them.[214] The *Maxwell* court then stated that "[i]n the modern age of communications, society must recognize such expectations of privacy as reasonable. We believe such recognition is implicit in the Electronic Communications Privacy Act."[215] However, instead of expounding on these statements or explicitly making the connection between privacy expectations and the ECPA, the *Maxwell* court resumed its two-prong analysis under the Fourth Amendment.[216]

V. PROPOSAL

Searches conducted under Title III are more intrusive than traditional

210. *See supra* text accompanying notes 179-82.

211. Any communication satisfying the definition of wire or electronic communication is protected by the ECPA unless it is *specifically* excluded in the definition. *Compare* 18 U.S.C. § 2510(1) (defining wire communication) *with* 18 U.S.C. § 2510(12) (defining electronic communication with specific exceptions). *Cf.* S. REP. NO. 541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3569 (explaining that electronic communications readily accessible to the general public are excluded).

212. *See* United States v. Maxwell, 42 M.J. 568, 576 (C.M.A. 1995).

213. *Id.*

214. *Id.*

215. *Id.*

216. *Id.*

government searches.[217] To maintain the balance between law enforcement and individual rights required under the Fourth Amendment, electronic and wire searches warrant greater protections.[218] One way to further this proposition is for courts to take the *Maxwell* approach one step further by accepting that the inclusion of a communication in the ECPA is indeed probative of a reasonable expectation of privacy.[219] Congressional action that offers a greater protection to a communication technology is indicative of society's readiness to find that the user of such a communication holds a reasonable expectation of privacy.

Courts can take this one step further and deem inclusion of a technology under the ECPA to show per se an objective privacy expectation.[220] Under this theory, a finding that a communication technology fits under the definition of electronic communication would satisfy the objective prong of the *Katz* two-prong test under a Fourth Amendment analysis.[221] Adherence to this theory prevents a court from separately finding that the user lacked a reasonable expectation of privacy in the communication to deny suppression.[222]

---

217. CARR, *supra* note 83, at § 2.5(a). Electronic searches are more intrusive than traditional searches because an electronic search usually affects more people, lasts longer, and is conducted in secrecy, whereas the subject of a traditional search knows either simultaneously or immediately after that a search occurred. *Id. See also* Askin v. McNulty, 47 F.3d 100, 105 (4th Cir. 1995) (describing the tension between more intrusive uses of technology, personal privacy, and the fight against more sophisticated criminal activity), *cert. denied*, 116 S. Ct. 382 (1995).

218. CARR, *supra* note 83, at § 2.5(a). Carr suggests electronic searches should ellicit a greater degree of court scrutiny than traditional searches because of the "secretive, intrusive, and indiscriminately acquisitive nature of electronic surveillance," but notes that courts do not provide such heightened protection. *Id.*

Technological innovations, however, may actually *increase* an individual's expectation of privacy. For instance, encrypting data transmissions heighten the level of security of that transmission by dramatically decreasing the ability to intercept it.

219. *See supra* notes 179-86 and accompanying text.

220. *Contra* United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992). The *Smith* court warns against creating a general rule regarding the reasonableness of an individual's privacy expectations, and explains that "[t]he creation of such a general rule . . . is beyond the proper role of the judiciary." *Id.*

221. This theory may, however, contradict legislative intent manifested by section 2515. *See* 18 U.S.C. § 2515 (1994). Since section 2515 only prohibits introduction of evidence obtained from oral or wire communications, the legislative intent may be to disallow the suppression of evidence obtained from electronic communications under the ECPA. *Id.*

222. *See Askin*, 47 F.3d at 105-06. The court expressed relief at finding it unnecessary to determine whether a communication technology specifically excluded from the ECPA is, nonetheless, protected by the Fourth Amendment, and warned courts to take "cautio[n] not to wield the amorphous 'reasonable expectation of privacy' standard in a manner that nullifies the balance between privacy rights and law enforcement needs struck by Congress in Title III." *Id.* (citations omitted)

Under either proposed theory, inclusion within the ECPA is relevant only to the objective prong of the *Katz* two-prong analysis.[223] A court must still find the user held a subjective expectation of privacy in the intercepted communication.[224] Once a court finds the communicator held a subjective expectation of privacy in a communication protected by the ECPA, then a holding of an unlawful interception justifies suppression.

A corollary to this proposal is that the specific exclusion of a communication from the ECPA is probative that the particular communication technology lacks a reasonable expectation of privacy for Fourth Amendment analysis. As the *Maxwell* approach assumes the legislature included a specific communication technology because its user would hold a justifiable expectation of privacy, the specific exclusion of a technology is probative of the contrary assumption.[225]

The mere absence of a particular technology from the ECPA, in contrast to the specific exclusion of a particular technology, should not, however, fall within this corollary. In other words, the absence of a communication technology in the ECPA definitions is not probative of any reasonable expectation of privacy for Fourth Amendment purposes. This approach addresses the continuous changes and growth in communications technology.

This proposal does not provide unlimited protection from any government searches and seizures of modern communication technologies. Showing reasonable cause, obtaining a search warrant, and following the procedures in section 2516 will still authorize the government to search and seize electronic, wire, and oral communications.[226]

223. See *supra* text accompanying notes 57-62 for a discussion of the objective prong of the *Katz* two-prong analysis.

224. See *supra* text accompanying notes 51-56 for a discussion of the subjective prong. Although the subjective prong is part of the *Katz* test, other courts have stated that it is the objective prong of the *Katz* test that controls. *See supra* note 57.

225. Under this corollary, the *Smith* court would not have undertaken a separate Fourth Amendment analysis once the conclusion was reached that cordless phones are specifically excluded from the ECPA. *See* United States v. Smith, 978 F.2d 171 (5th Cir. 1992).

226. *See* 18 U.S.C. §§ 2515 to 2522 (1994).

VI. CONCLUSION

As the realm of communications technology continues to expand, new questions regarding the privacy expectations of a user of such technology will continue to confront courts in suppression hearings resulting from wiretaps.[227] Although the Fourth Amendment will always provide a baseline level of protection against overzealous law enforcement, Congress has contributed to Fourth Amendment protections through the enactment of the ECPA and other statutes.[228] Courts have used different approaches to balance these Congressional statutes and Fourth Amendment privacy rights.[229] A more expansive reading by the courts of the ECPA regarding privacy expectations will prevent traditional Fourth Amendment search analyses from contravening the privacy implications within the ECPA.[230] Holding that a communication technology that is protected by the ECPA is probative, or even conclusive of an objectively reasonable expectation of privacy, can still advance the government's goals of combatting crime and concomitantly upholding an individual's constitutional rights.[231]

MICHELLE SKATOFF-GEE

227. See *supra* notes 1-24 and accompanying text introducing the problem of changing technologies in the context of the Fourth Amendment.

228. *See supra* Part II.C.

229. *See supra* Part III.

230. *See supra* Part IV.

231. *See supra* Part V.