Volume 33
Number 1 *Fall 1998*

*pp.*231-274

*Fall 1998*

# Keeping "Private E-Mail" Private: A Proposal to Modify the Electronic Communications Privacy Act

Robert S. Steere

# KEEPING "PRIVATE E-MAIL" PRIVATE: A PROPOSAL TO MODIFY THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

*I am not an advocate for frequent changes in laws and institutions. But laws and institutions must go hand-in-hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths discovered and manners and opinions change, with change of circumstances, institutions must advance also to keep pace with the times.*[1]

## I. INTRODUCTION

Our present society has expanded tremendously because the Internet links people via computers in a way that creates the perception that no physical distance separates people who communicate in cyberspace.[2] One of the infinite uses of cyberspace is the transmission of electronic mail, or e-mail.[3] E-mail is essentially the core of on-line activity, because it comprises the most common, basic function that allows individuals to correspond with one another via computers.[4] Although most citizens consider the right of privacy, such as a citizen's right of privacy in his or her e-mail, as a fundamental right, the United States Constitution does not enumerate privacy as a protected right.[5]

---

[1] Letter from Thomas Jefferson to Samuel Kercheval (1816).

[2] Cyberspace was first coined in a novel by WILLIAM GIBSON, NEUROMANCER (1980). Cyberspace describes the matrix of interconnected computers on the Internet that allows people with a personal computer to connect and communicate even though they are hundreds of miles or even thousands of miles apart. In the future, millions of Americans will benefit from the High-Performance Computing Act passed in 1991. Congress designed the federal legislation to bolster the development of a digital information infrastructure. High-Performance Computing Act of 1991, 15 U.S.C.A. §§5501-5528 (West 1998).

[3] *See* JACOB PALME, ELECTRONIC MAIL 1 (1995).

[4] *Id.* at 4. "The user produces, sends, and usually also receives mail at a . . . personal computer." *Id.*

[5] Although the Constitution does not enumerate privacy as a protected right, the Court in *Camara v. Municipal Court*, explained that:

> The basic purpose of [the Fourth] Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by government officials. The Fourth Amendment thus gives concrete expression to a right of the people which 'is basic to a free society.

Camara v. Municipal Court, 387 U.S. 523, 528 (1967) (quoting Wolf v. Colorado, 338 U.S. 25, 27 (1949)).

Therefore, e-mail privacy rights, recognized by today's courts, derive their primary authority from the Electronic Communications Privacy Act ["ECPA"] of 1986[6] and the Fourth Amendment to the Constitution which specifically prohibits unreasonable searches and seizures.[7] These privacy rights play a unique role in the American law that is so vital to any free society.[8] Legislators and judges must protect our most basic and fundamental personal freedom even though computers and digital communication technologies present a serious challenge to law enforcement.[9] To maintain a proper balance between the needs of society and citizens' civil liberties, the American legal system must constantly react to emerging technologies.[10]

Keeping in mind the need for the law to react, this Note has a dual purpose. First, the Note suggests that the Supreme Court has yet to capture the true essence of the Fourth Amendment and instead has strayed from the historical purpose of the Amendment.[11] Second, the

---

[6] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of Title 18 of the United States Code).

[7] The Fourth Amendment to the United States Constitution provides:

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

U.S. CONST. amend. IV.

[8] *See* Lloyd L. Weinreb, *Generalities of the Fourth Amendment*, 42 U. CHI. L. REV. 47, 85 (1974) ("The privacy secured by the Fourth Amendment fosters large social interests. Political and moral discussion, affirmation and dissent, need places to be born and nurtured, and sheltered from unwanted publicity"). *See also* Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 388 (1974) (noting that citizens' knowledge that each is free to express himself or herself freely "is the hallmark of an open society"). In contrast, privacy's antithesis, "police omniscience[,] is one of the most effective tools of tyranny." Lopez v. United States, 373 U.S. 427, 466 (1963) (Brennan, J., dissenting).

[9] *See* Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 735 (1988) ("The Fourth Amendment absolutely requires a continuous supervision by the judiciary [and the legislature] over law enforcement. For the Court [or Congress] to do any less than this, is to fail in . . . [their] responsibility to the Framers of the Constitution and to the citizenry").

[10] Professor Gutterman argues that "[u]nrestrained, over time, technology can steadily erode our privacy protections, thus making our society terribly oppressive." *Id.*

[11] Many scholars criticize the Court's Fourth Amendment jurisprudence. *See, e.g.*, Amsterdam, *supra* note 8, at 349 (stating that the Court's Fourth Amendment jurisprudence is not its "most successful product"); Clark D. Cunningham, *A Linguistic Analysis of the Meanings of "Search" in the Fourth Amendment: A Search for Common Sense*, 73 IOWA L. REV. 541, 543 (1988) (stating that the majority of scholars agree that the Court's Fourth Amendment "search" cases "[do] not make sense"); Roger B. Dworkin, *Fact Style*

Note argues that Congress's enactment of the ECPA to protect e-mail also fails to provide enough protection to satisfy the true historical purpose of the Fourth Amendment.

Section II of this Note analyzes the historical purpose of the Fourth Amendment and traces the development of the current privacy doctrine enunciated in the Court's seminal "search" case, *Katz v. United States.*[12] Section III explores the post-*Katz* sub-doctrines to demonstrate that these cases misapply the true spirit of the *Katz* doctrine and divert attention from the historical purpose of the Fourth Amendment.[13] Section IV of this Note explores the nature of the Internet and electronic mail.[14] Section V examines whether an "electronic communication," such as a private e-mail, receives enough protection, under the ECPA, to satisfy the historical purpose of the Fourth Amendment in comparison to a "wire" or "oral" communication.[15] The section ultimately determines that the formalistic distinctions, which result from Congress's failure to sufficiently distinguish an "electronic communication" in "transit" from an "electronic communication" held in "electronic storage," should mandate reformed legislation. Finally, Part VI of this Note proposes modifications to update the ECPA whereby the ECPA provides equal privacy protection to all communications, especially an "electronic communication," in order to encourage the growth and use of emerging communication technologies.[16]

---

*Adjudication and the Fourth Amendment: The Limits of Lawyering*, 48 IND L.J. 329, 329-30 (1973) (stating that "[t]he Fourth Amendment cases are a mess!").

[12] 389 U.S. 347 (1967). *See infra* notes 18-66 and accompanying text.

[13] *See infra* notes 68-86 and accompanying text.

[14] *See infra* notes 89-100 and accompanying text.

[15] *See infra* notes 103-227 and accompanying text.

[16] *See infra* notes 230-54 and accompanying text.

## II. THE FOURTH AMENDMENT

### A. The Historical Purpose of the Amendment

> *[I] think it a less evil that some criminals should escape than that the government should play an ignoble part [in gathering evidence].*[17]

The Fourth Amendment to the United States Constitution has a rich historical background rooted in American, as well as English, law.[18] The Amendment is the one procedural safeguard in the Constitution that grew directly out of the events that preceded the revolutionary struggle with England, particularly the colonial protest against writs of assistance and general warrants.[19] As a response to these unreasonable law enforcement practices employed by agents of the British Crown, the Framers of the Constitution included the Fourth Amendment in the Bill of Rights[20] to restrain executive power.[21] Acting as a bulwark against police practices that prevail in a totalitarian government,[22] the Fourth Amendment protects citizens from government agents[23] who conduct

---

[17] Olmstead v. United States, 277 U.S. 438, 470 (1928) (Oliver Wendell Holmes, Jr., dissenting). *Olmstead*, which involved wiretapping of a bootlegger, was finally overturned in the 1967 *Katz* decision where the Supreme Court held that government agents had to obtain a court order to place wiretaps. Olmstead v. United States, 277 U.S. 438, 470 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

[18] For the specific text of the Fourth Amendment, see *supra* note 7.

[19] For a detailed analysis about the historical purpose of the Fourth Amendment, see JACOB W. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT: STUDY IN CONSTITUTIONAL INTERPRETATION 19-20 (1966). Writs of assistance were judicial orders, which authorized officers of the Crown to enter and search buildings for smuggled goods. *Id.* at 31-32. General warrants were employed to enforce seditious libel laws by granting royal officers the authority to search out and seize writings that were critical to the Crown. *Id.* at 21.

[20] The drafters of the Bill of Rights intended that it act as a limitation on the federal government only, but the Fourth Amendment is applicable to the states through the Due Process Clause of the Fourteenth Amendment which was adopted in 1868. *See also* Smith v. Maryland, 59 U.S. 71 (1855) (recognizing that the Bill of Rights only limits the federal government); Wolf v. Colorado, 338 U.S. 25, 27-28, 33 (1949) (recognizing that the Fourth Amendment applies to the states). *See, e.g.*, Boyd v. United States, 116 U.S. 616, 626-27 (1886) (stating that the practice of writs of assistance and general warrants explained the nature of the proceedings intended by the Fourth Amendment).

[21] *See* California v. Acevedo, 500 U.S. 565, 586 (1991) (Stevens, J., dissenting); Weeks v. United States. 232 U.S. 383, 389-391 (1914); Boyd v. United States, 116 U.S. 616, 624-25 (1886); 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE §§ 3-5 (2d ed. 1987).

[22] *See Acevedo*, 500 U.S. at 586 (explaining that the Fourth Amendment acts as a wall against a government that oppresses opposition).

[23] *See* Burdeau v. McDowell, 256 U.S. 465 (1921) (recognizing that evidence illegally obtained by a private party acting independently of police direction will not be excluded).

unreasonable[24] searches[25] and seizures.[26] However, the drafters left the enforcement of the Fourth Amendment unsettled.[27]

The Fourth Amendment contains no language setting forth the consequences in the event that the government violates the Amendment's strictures.[28] However, over the course of the last century, the United States Supreme Court concluded that the best method to enforce the Fourth Amendment in criminal prosecutions was to forbid the government from using evidence obtained in violation of the

---

[24] *See* United States v. Brignoni-Ponce, 422 U.S. 873, 878 (1975) (maintaining that reasonableness "depends on a balance between the public interest and the individual's right to personal security free from arbitrary interference by law officers"); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652-53 (1995) (quoting Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 619 (1989)) (the reasonableness of a particular law enforcement practice is judged by "balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate government interests"); Terry v. Ohio, 392 U.S. 1, 19 (1968) (recognizing that the touchstone of the Fourth Amendment is the "reasonableness in all the circumstances of the particular government invasion of a citizen's personal security").

[25] *See* Katz v. United States, 389 U.S. 347 (1967) (holding that a search occurs when government action intrudes into an area where a person has a reasonable and justifiable expectation of privacy). For a detailed discussion of the *Katz* decision, see *infra* notes 55-64 and accompanying text.

[26] *See* United States v. Mendenhall, 446 U.S. 544 (1980) (holding that seizure of a person occurs, when under the totality of the circumstances, "a reasonable person would have believed that he was not free to leave" when confronted by a government agent). *See also* California v. Hodari D., 499 U.S. 621, 626 (1991) (expanding the seizure definition to include a government agent's use of physical force or a person's submission to a government agent's assertion of authority).

[27] *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 1.1(a), at 5-6 (3d ed. 1996) (explaining that, unlike the Fifth Amendment, no mention is made barring from evidence the fruits of a violation of the Fourth Amendment).

[28] *Id.*

Amendment.[29] Thus, the "exclusionary rule" evolved to deter government agents from violating the Fourth Amendment.[30]

### B. *The Development of the* Katz *Standard*

*Civilization is the progress toward a society of privacy.*[31]

While the Supreme Court formulated the "exclusionary rule" to protect people against evidence gathered in violation of the Fourth Amendment,[32] the Court did not explain what constituted a violation. Although the British government's blatant physical intrusions initiated the right to be free from unreasonable searches and seizures,[33] the Supreme Court's first major Fourth Amendment case, *Boyd v. United States*,[34] did not involve a physical trespass at all.[35] In *Boyd*, the issue

---

[29] Over a hundred years ago, the Supreme Court began evolving the most effective means of enforcing the Fourth Amendment. As a result, the "exclusionary rule" now bars the use in federal or state court criminal proceedings of evidence that a federal or state government obtains in violation of the Fourth Amendment. *See* Boyd v. United States, 116 U.S. 616 (1886) (excluded evidence in federal court that the federal government obtained by violating the Fourth Amendment); Weeks v. United States, 232 U.S. 383 (1914) (excluded evidence in federal court—but not state court—when a federal agent partook in an action that violated the Fourth Amendment); Wolf v. Colorado, 338 U.S. 25 (1949) (holding that victims whose Fourth Amendment rights were violated by the state must rely on state remedies), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961) (holding that all evidence obtained by searches and seizures in violation of the Constitution is inadmissible in a state court).

[30] The "exclusionary rule" operates as a deterrent to government agents who violate the Fourth Amendment by excluding evidence seized as a result of such conduct, but not as a punishment to government agents for the errors of judges and magistrates. Nevertheless, the exclusionary rule is subject to exceptions such as the "good faith" exception. The Supreme Court enunciated the "good faith" exception in *United States v. Leon*, when the Court held that evidence that the government obtained in reasonable reliance on a facially valid warrant may be used by the prosecution, despite an ultimate finding that the warrant was not supported by probable cause. United States v. Leon, 468 U.S. 897, 913 (1984). In *Leon*, a neutral and detached magistrate approved a police officer's application for a search warrant based on information from a confidential informant. *Id.*

[31] AYN RAND, THE FOUNTAINHEAD 7 (1943).

[32] For a private civil cause of action based on a Fourth Amendment violation, see Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971) (providing a citizen a cause of action for monetary damages upon proof of injuries, resulting from a search conducted by federal agents in violation of the Fourth Amendment).

[33] *See supra* notes 18-30 and accompanying text.

[34] 116 U.S. 616 (1886). The only case decided before *Boyd* of any significance was *Ex parte Jackson*, where the Court required, in dictum, that the government obtain a warrant before opening a sealed letter sent through the mail. *Ex Parte* Jackson, 96 U.S. 727, 733 (1877).

[35] *Boyd*, 116 U.S. at 619-20. In *Boyd*, the case was not even a criminal proceeding but a civil forfeiture proceeding where the government claimed that the Boyd partnership fraudulently evaded paying custom duties on imported plate glass. *Id.* at 617-18. A court

concerned the constitutionality of a federal statute which provided that, in certain non-criminal cases, the court may require the production of a person's private papers if the government asserts that the evidence would help prove a certain allegation.[36] The Supreme Court held that this mandatory production of certain papers violated the Fourth and Fifth Amendments.[37] Compelling persons to be witnesses against themselves by using a subpoena to force the production of wanted papers, the Court reasoned, was no different from the government merely seizing the papers.[38] The method used by the government to obtain the papers as evidence was not the essence of the offense.[39] Instead, the essence was the invasion of a person's right of personal security, personal liberty, and private property implicit in the history of Fourth Amendment protection.[40] Although the *Boyd* Court took an important step by placing a unique value on the nature of the privacy right,[41] the Court's progressive construction of the Fourth Amendment was short-lived. Two subsequent cases required that a constitutionally "protected area" be "physically trespassed" by the government before Fourth Amendment protection could be triggered.[42]

---

order, obtained through the forfeiture proceedings, required the partnership to produce certain invoices that the government planned to use as evidence to prove tax evasion. *Id.*

[36] *Id.* at 620. The Court stated that "[i]t is not the breaking of . . . doors," and "rummaging of . . . drawers, that constitutes the essence [of a Fourth Amendment violation], but it is the invasion of [a person's] indefeasible right of personal security, personal liberty, and private property" which calls the Fourth Amendment into question. *Id.* at 630. The Court explained that it was not the existence of a physical trespass that made the government's practices so despicable. *Id.*

[37] *Id.* The Court held that the Fourth Amendment sought to prohibit the government from wielding arbitrary power and from compelling a person to produce incriminating papers without cause, because the procurement was merely an insidious disguise of an old practice that the founding fathers deeply abhorred. *Id.* The Court also noted that the Fourth Amendment condemns unreasonable searches and seizures, because the Fifth Amendment condemns the government from compelling persons to produce evidence against themselves. *Id.* at 633. For the text of the Fourth Amendment, see *supra* note 7. The Fifth Amendment states in pertinent part: "No person . . . shall be compelled in any criminal case to be a witness against himself . . . ." U.S. CONST. amend. V.

[38] *Boyd*, U.S. 116 at 633.

[39] *Id.* at 630.

[40] *Id.*

[41] *See* Gutterman, *supra* note 9, at 649 (explaining that "Boyd chartered a course that placed the Fourth Amendment upon a 'value-dominated model'").

[42] *See* Hester v. United States, 265 U.S. 57, 58 (1924) (holding that when the police entered defendant's open field to obtain evidence, they did not violate the Fourth Amendment, because the special protection accorded to people in their houses does not extend to open fields); Olmstead v. United States, 277 U.S. 438, 464 (1928) (holding that police interception of telegraph messages did not constitute a Fourth Amendment violation because oral

In *Hester v. United States*[43] and in *Olmstead v. United States*,[44] the Court retreated from its prior holding in *Boyd* and relied on twin principles to test the confines of the Fourth Amendment.[45] The first principle, embraced by the Court in *Hester*, was the "protected areas" standard in which the Court strictly construed the literal language of the Amendment to mean that a governmental trespass onto a citizen's open field did not constitute a "search."[46] The second principle, embraced by the Court in *Olmstead*, was the trespass-oriented standard whereby the Court decided that the government could conduct warrantless taps on a defendant's telephone to intercept and listen to telephone conversations if the government did not physically trespass into the defendant's home or office.[47] The *Olmstead* Court reasoned that the Fourth Amendment is only concerned with the government's blatant physical intrusions and not the mere interception of telephone conversations.[48] Conversations

---

communications were not the type of tangibles that the Fourth Amendment sought to protect).

[43] 265 U.S. 57 (1924). In *Hester*, the government charged the defendant with concealing distilled spirits, as well as other liquor-related offenses, in violation of a revenue statute. *Id.* The government obtained its evidence by entering the defendant's open field, some 50 to 100 yards away from the house where the defendant lived. *Id.* at 58. From this vantage point, the government saw the defendant in possession of what appeared to be, and what was later confirmed as, a jug of whiskey. *Id.* The defendant challenged the government's conduct, arguing that the government conducted an illegal search. *Id.* The Court rejected the argument and held that no search occurred because the government only entered upon the defendant's open field. *Id.* at 58-59. Generally, this is referred to as the "open fields" doctrine. *See infra* notes 76-79 and accompanying text.

[44] 277 U.S. 438 (1928). In *Olmstead*, the government charged the defendants with conspiracy to violate the National Prohibition Act because they dealt with intoxicating liquors. *Id.* The government obtained its evidence by intercepting messages from four of the defendants' residences. *Id.* at 456-57. The government intercepted these messages by inserting telephone wiretaps, but did not trespass onto any of the defendants' property. *Id.* at 457. *Olmstead* is arguably the Court's first foray into cyberspace jurisprudence. Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-wide Search*, 105 YALE L.J. 1093, 1102 (1996).

[45] *See* Bruce G. Berner, *The Supreme Court and the Fall of the Fourth Amendment*, 25 VAL. U. L. REV. 383 (1991). Professor Berner explained the two-part "search" doctrine prior to 1967: First, *Hester* held that the "place" must be one that the Fourth Amendment is concerned with; and second, *Olmstead* held that the government action must be one that the Fourth Amendment scrutinizes—physical trespass. *Id.*

[46] The Court explained that "the special protection afforded by the Fourth Amendment to the people in their 'persons, houses, papers and effects,' is not extended to . . . open fields." *Hester*, 265 U.S. at 59.

[47] *Olmstead*, 277 U.S. at 464. The Court decided that the Fourth Amendment was not concerned with telephone conversations because they were not tangible. *Id.*

[48] *Id.* at 463-66. The Court argued that the framers of the Constitution meant to protect an individual's privacy interest only in regards to those physical items mentioned specifically in the Amendment: their persons, houses, papers, and effects. *Id.* at 463. With this principle in mind, the Court proclaimed that:

passing over telephone wires, the Court decided, were not the material kinds of things that the Fourth Amendment protected if the means the government used to obtain these conversations did not physically invade a "protected area."[49]

Writing for the dissent in *Olmstead*, Justice Brandeis refused to adopt the majority's literal construction of the Fourth Amendment. Justice Brandeis wanted the Court to follow the *Boyd* precedent, whereby the Court refused to limit Fourth Amendment protection from applying to the means used by the government to invade upon a citizen's "right to be let alone."[50] According to Justice Brandeis, the true essence of Fourth Amendment protection guarantees citizens that right of privacy.[51] Justice Brandeis further explained that, at the time our Founding Fathers adopted the Constitution, force and violence were the only ways for the government to procure evidence directly from a defendant. But he emphasized that time works change.[52] What the framers of the Constitution could not, and did not, address was the myriad of privacy concerns that developed as society introduced new technologies that

---

> The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the house, or offices of the defendant.

*Id.* at 464.

[49] *Id.* at 464-65. The Court reiterated that "[t]he amendment itself shows that the search is to be of material things—the person, the house, his papers, or his effects." *Id.* at 464. Applying this principle, the Court asserted that "[t]he language of the amendment cannot be extended and expanded to telephone wires, reaching to the whole world from the defendant's house or office." *Id.* at 465.

[50] *Olmstead* v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). *See also* Gutterman, *supra* note 9, at 658-59.

[51] Justice Brandeis looked back upon the historical purpose of the Fourth Amendment and commented:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

*Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting). For the specific text of the Fourth Amendment, see *supra* note 7.

[52] *Olmstead*, 277 U.S. at 474.

enabled the government to expose the most intimate occurrences of citizens without physical intrusion, force, or violence.[53]

### C. *The* Katz *Decision: The Reasonable Expectation of Privacy Standard*

> *The right to be let alone—the most comprehensive of rights and the right most valued by civilized men.*[54]

In light of Justice Brandeis's reasoning, which focused on the historical purpose behind the Fourth Amendment's implicitly guaranteed right of privacy, the Court eventually overruled the notion that only a physical trespass into a narrowly defined list of places would constitute a "search."[55] In the seminal "search" case, *Katz v. United States*,[56] both parties' attorneys tailored their respective arguments to coincide with the precedent set forth in *Hester* and *Olmstead*,[57] but the Court decided to dismantle its traditional twin-principle trespass test and established a new principle to define the Fourth Amendment right to be free from unreasonable searches.[58] The new principle that resulted to

---

[53] Justice Brandeis stated that:

> in the application of a Constitution [the Court's] contemplation cannot be only of what has been but of what may be. The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. 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.

*Id.*

[54] *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).

[55] *See* Berner, *supra* note 45 and accompanying text, for a summary of the two-part test based on *Hester* and *Olmstead* which the Court relied on during this era. For a list of places that would constitute a search subject to Fourth Amendment scrutiny prior to 1967, *see* Berner, *supra* note 45 at 386 n.11.

[56] 389 U.S. 347 (1967). In *Katz*, the defendant made a telephone call in a public telephone booth to allegedly make an illegal wagering transaction. *Id.* at 348. FBI agents placed an electronic recording device on the outside of the booth to record the defendant's conversation in order to obtain evidence to indict the defendant for violating a federal statute which prohibited the transmittal of wagering information by telephone. *Id.* The FBI agents placed the recording device on the outside of the telephone booth, so that no physical invasion occurred into an area that the defendant occupied. *Id.* at 348-49.

[57] The attorneys in *Katz* argued over whether a telephone booth was the type of "protected place" accorded protection by the Fourth Amendment and whether placing the electronic recording device on the outside of the telephone booth constituted an actual trespass. *Id.* at 349-51. For a discussion of the two-part trespass test, promulgated in *Hester* and *Olmstead*, used prior to *Katz*, *see* Berner, *supra* note 45 and accompanying text.

[58] The Court rejected the first principle, set forth in *Hester*, that the Fourth Amendment applied only to a relatively short list of protected places and recognized that the Fourth Amendment "protects people—and not simply 'areas'—against unreasonable searches and seizures," regardless of the absence or presence of a physical intrusion. *Katz*, 389 U.S. at

analyze whether a defendant may invoke the Fourth Amendment in connection with a particular set of facts was whether the person affected had a reasonable expectation of privacy with regard to the activity intruded upon.[59]

While the majority of the Court adopted this new principle for defining a "search" under the Fourth Amendment, the language found in Justice Harlan's concurring opinion emerged as the foundation for the "reasonable expectation of privacy" test that exists today.[60] Justice Harlan broke his test into two parts: 1) a person must 'exhibit' an actual or subjective, expectation of privacy;[61] and 2) society must be objectively prepared to recognize that expectation as reasonable.[62] The purpose of this new doctrine was to escape the formalistic structure of the prior property-based analysis and to instead declare that the Fourth Amendment protects privacy rights which society accepts as reasonable.[63]

---

353. The Court then rejected the second principle, set forth in *Olmstead*, that the Fourth Amendment only protects against actual physical trespasses, recognizing that the Fourth Amendment protects a person's justifiable expectation of privacy regardless of whether the government made an actual physical trespass. *Id.*

[59] The *Katz* Court reasoned that:

> [The defendant] did not shed his [Fourth Amendment] right simply because he made his calls from a place from where he might be seen. . . . One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcasted to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

*Id.*

[60] *Id.* at 361.

[61] *Id.* The subjective prong requires that individuals take actual affirmative steps to "exhibit" their intention to ensure their privacy. *Id.* Some commentators contend that the "inquiry into the particular defendant's subjective state of mind has no place in the application of the *Katz* expectation of privacy standard." LAFAVE, *supra* note 21, § 11.3(c), at 157.

[62] *Katz*, 389 U.S. at 361 (Harlan, J., concurring). The objective prong ensures that expectations of privacy are reasonable. *Id.* For example, a person cannot expose something to the "plain view" of outsiders, yet claim Fourth Amendment protection by asserting a subjective expectation of privacy. *Id.*

[63] *See* Gutterman, *supra* note 9, at 663. Professor Gutterman explained the intended effect of the new doctrine this way:

> This view of the fourth amendment was intended to escape the structure of a formalistic property analysis and to affirm the concept that the amendment protects certain property rights. . . . The right of the individual to be left alone to live his daily life secure against

While the *Katz* doctrine expanded the Fourth Amendment's protection of privacy rights by broadening the scope of what constituted a "search," the doctrine is inherently limited, because it requires an individual to form an expectation of privacy and take precautions to ensure that privacy.[64] By focusing on a defendant's lack of objective manifestation to protect his privacy, the Court, increasingly concerned with law and order,[65] created sub-doctrines which insulated law enforcement from review when the precautions that the defendant took to ensure his privacy were insufficient to earn privacy.[66]

## III. SUB-DOCTRINES THAT LIMIT THE *KATZ* DOCTRINE

> *If the Constitution is to be construed to mean what the majority at any given period in history wish the Constitution to mean, why a written Constitution and deliberate process of amendment?*[67]

Since 1967, the Court has limited the *Katz* "reasonable expectation of privacy" doctrine and has effectively reduced the ambit of Fourth Amendment privacy. In other words, even if a person has a "reasonable expectation of privacy," certain exceptions may override that

---

> arbitrary invasions by government officials appeared once again to become the basic value protected by the Fourth Amendment.

*Id.*

[64] *See Katz*, 389 U.S. at 361 (requiring that an individual form an expectation of privacy to trigger his Fourth Amendment right to be free from unreasonable searches and seizures). *See also* Gutterman, *supra* note 9, at 664 (explaining that the Fourth Amendment protected Katz's telephone conversation not only because the Court decided that society places a value on a telephone conversation that entitled him privacy but also because Katz took self-protective steps to ensure his privacy).

[65] *See, e.g.*, Maryland v. Wilson, 117 S. Ct. 882 (1997) (holding that a law enforcement officer making a traffic stop may order passengers out of the car pending completion of the stop).

[66] The problem with Justice Harlan's two-part test is that a court has no way of determining whether a defendant has a subjective expectation of privacy other than by determining whether the defendant made any objective manifestations to ensure his privacy. Professor Gutterman explains:

> [A] right dependent upon subjective expectations could make the fourth amendment's application too dependent upon a finding of objective measures used to protect privacy. . . . Moreover, by manipulating the importance of the objective factors manifesting privacy expectations, focus could be deflected from the content of the amendment's privacy values to the risk of exposure in failing to take precautions to protect these values.

Gutterman, *supra* note 9, at 666.

[67] Frank J. Hogan, PRESIDENTIAL ADDRESS AT THE AMERICAN BAR ASSOCIATION CONVENTION, SAN FRANCISCO (July 10, 1939).

expectation. An analysis of these post-*Katz* cases is necessary to understand the problems associated with legislating and judicially enforcing laws to protect e-mail privacy.

### *A. The Standing Doctrine*

A citizen may not exclude evidence from a criminal proceeding under the "exclusionary rule"[68] based upon a purported violation of someone else's rights because the Fourth Amendment right to privacy is personal.[69] Although a straightforward rule for assessing whether the government violated a defendant's personal Fourth Amendment right cannot be stated, the Court's leading standing case is *Rakas v. Illinois*.[70] In *Rakas*, the Court retreated from its holding in *Jones v. United States*[71] by deciding that a defendant may assert Fourth Amendment rights as to those areas or objects in which the person has a "legitimate expectation of privacy."[72] To determine whether a person has a "legitimate expectation of privacy," the Court objectively asked whether the defendant had the power to exclude others by exercising dominion and

---

[68] For an explanation of the "exclusionary rule," see *supra* notes 27-30 and accompanying text.

[69] *See* WAYNE R. LAFAVE & JEROLD ISREAL, CRIMINAL PROCEDURE § 9.1, at 459-60 (1992) (explaining that Fourth Amendment rights are personal rights that may not be asserted vicariously). Standing is a very important inquiry for e-mail privacy because two parties, a sender and a receiver, communicate together. If the government intercepted a private e-mail communication, then both parties have standing to object to the admission of the communication into evidence under the "exclusionary rule." Alderman v. United States, 394 U.S. 165, 176 (1969) (explaining that during a telephone conversation, both parties have standing to object to a wiretap). A party may lack standing to object to the admission of an e-mail communication into evidence when one party either consented to the disclosure of the e-mail to the government or disclosed the e-mail as a result of an illegal search and seizure by the government. *See* United States v. Payner, 447 U.S. 727, 731-32 (1980). *See also infra* notes 81-83 and accompanying text (discussing the "assumption of the risk" doctrine).

[70] 439 U.S. 128 (1978). In *Rakas*, the police stopped an automobile and ordered the occupants to exit. *Id.* at 130. A search of the automobile, conducted without a search warrant and without probable cause, revealed a rifle under the seat and shells in the glove compartment. *Id.* The Court denied the defendant, a passenger, standing to challenge the illegal search because he was not the owner or driver of the car and had no ownership or possessory interest. *Id.*

[71] 362 U.S. 257 (1960), *overruled by* United States v. Salvucci, 448 U.S. 83 (1980). In *Jones*, a police search of an apartment, without a search warrant and without probable cause, revealed contraband. *Id.* at 259. The Court granted the defendant, a guest, standing to challenge the illegal search because he was "legitimately on [the] premises" at the time of the search. *Id.* at 267. *See also* Rawlings v. Kentucky, 448 U.S. 98 (1980).

[72] The Court borrowed language from *Katz* and stated that "the Fourth Amendment depends not upon a property right in the invaded place but upon whether the person who claims the protection of the amendment has a legitimate expectation of privacy in the invaded place." *Rakas*, 439 U.S. at 143.

control.[73] The Court reasoned that the right to exclude others invariably stems from the ownership or lawful possession of real or personal property.[74] As the Court incorporated this doctrine and additional doctrines, it severely limited the ambit of Fourth Amendment privacy protection.[75]

### B. *The Open Fields Doctrine*

The "reasonable expectation of privacy" test, espoused in *Katz*, stated in very certain terms that the Fourth Amendment protects people and not places.[76] But the Court, in *Oliver v. United States*,[77] followed the historical view,[78] which regarded any property outside the "curtilage" of the home as unprotected "open fields." In *Oliver*, the Court held that even if the police trespassed on private property that the owner fenced and posted with "No Trespassing" signs, their observations of activities or objects on that property outside the curtilage of the home was not a

---

[73] The Court asked whether the defendant had "complete dominion and control . . . and could exclude others from it." *Id.* at 149.

[74] *Id.* at 143-44 n.12. Unlike Jones who had a key, clothes in the closet and previously slept on the premises and unlike Katz who occupied the telephone booth, shut the door behind him to exclude others, and paid the toll, Rakas did not have any indicia of control to prove that he had a legitimate expectation of privacy to assert standing. *Id.* at 149.

[75] *See infra* notes 76-79 and accompanying text (discussing the Court's "open fields" doctrine).

[76] Katz v. United States, 389 U.S. 347, 351 (1967) (stating in clear language that the Fourth Amendment "protects persons, not places"). For a detailed analysis of the *Katz* decision, see *supra* notes 56-64 and accompanying text.

[77] 466 U.S. 170 (1984). In *Oliver*, narcotic agents trespassed onto Oliver's property, without a warrant, by walking around a locked gate marked with a "No Trespassing" sign. *Id.* at 173. The search revealed a field of marijuana about one mile outside the curtilage of the home. *Id. See also* United States v. Dunn 480 U.S. 294, 294-95 (1987) (applying four factors to determine whether an area is within the curtilage of the home: (1) the proximity of the area in question to the residence; (2) whether the area is included within an enclosure surrounding the entire home; (3) the nature of the uses to which the subject area is put; and (4) the steps taken by the resident to protect the area from observation). Thus, a barn located sixty feet from a house enclosed by a fence, not used for 'intimate activities of the home,' and not protected from observation by persons outside the home's fence, was not within the curtilage of the home and not the subject of a search when police looked inside. *Id.* at 295. For an explanation of the similar "plain view" doctrine whereby no Fourth Amendment violation occurs when lawfully present police officers view contraband or evidence of criminal activity from a vantage point which occasions no intrusion into the privacy of the suspect, see Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986); *see also* United States v. Place, 462 U.S. 696, 707 (1983) (extending the "plain view" doctrine by holding that the use of drug-sniffing dogs to detect the odor of narcotics in luggage is not a Fourth Amendment search).

[78] *See supra* note 42-46 and accompanying text (explaining the rule of *Hester* which provides that an individual may not legitimately demand privacy for activities conducted out of doors in open fields, except in the area immediately surrounding the home).

search within the operation of the Fourth Amendment.[79] Even though the effect of the Court's holding in *Oliver* gave law enforcement officers the power to trespass onto private property in "open fields," the Court continued to create an additional doctrine, making the *Katz* decision even more vacuous.[80]

### C. *The Assumption of the Risk Doctrine: Risk of Exposure*

While Justice Harlan's two-part test attempted to capture the essence of the majority decision in *Katz*, he based his test on a subjective expectation analysis stemming from an "assumption of the risk" theory.[81] The "assumption of the risk" doctrine suggests that a person might waive his Fourth Amendment protection when he exposes an object or activity to the general public.[82] The Supreme Court has held that citizens assumed the risk of exposure in numerous cases, particularly when the defendant conducted an activity outdoors or when a defendant voluntarily conveyed something to a third party.[83]

---

[79] *Id.* at 179. The court argued that neither "fences nor 'No Trespassing' signs effectively bar the public from viewing open fields . . . . [T]he asserted expectation of privacy in open fields is not an expectation that society recognizes as reasonable." *Id.*

[80] *See infra* notes 81-83 and accompanying text (discussing the "assumption of the risk" doctrine).

[81] *See* Gutterman, *supra* note 9, at 666-67.

[82] Professor Gutterman contends that while the Court formulated the *Katz* decision to accord technological developments with Fourth Amendment protection, thereby maintaining society's need for privacy, the risk assumption doctrine was the most significant factor in limiting the scope of the Fourth Amendment. *Id.* at 670.

[83] *See, e.g.*, Florida v. Riley, 488 U.S. 445, 449-52 (1989) (holding that when police used a helicopter to observe marijuana through the partially open roof and sides of a greenhouse, no "search" occurred because the general flying public could also observe the activity); California v. Greenwood, 486 U.S. 35, 40-42 (1988) (holding that the defendant's trash was not entitled to Fourth Amendment protection because the defendant placed it curbside where it was readily accessible to animals, scavengers, children, and snoops. The defendant placed it in a public area for the express purpose of having strangers take it away); United States v. Knotts, 460 U.S. 276, 281-82 (1983) (holding that no Fourth Amendment search occurs when an electronic device is attached to a vehicle in order to enable police to track its movement because a person driving in public has no reasonable expectation that movements of the vehicle will not be observed; the beeper does not intercept or divulge the contents on any communication); Smith v. Maryland, 442 U.S. 735, 742-44 (1979) (holding that because a defendant has no reasonable expectation of privacy that the telephone company will not disclose the telephone numbers he dials to the police, the use of pen registers to record the numbers dialed from a particular phone is not a search); United States v. Miller, 425 U.S. 435, 437 (1976) (holding that a bank depositor had no protectable Fourth Amendment interests in microfilm records of his financial transactions because by revealing his affairs to the bank, he assumed the risk that such information would be conveyed to the government). Congress, however, reversed the result in *Miller* in the Right to Financial Privacy Act, 12 U.S.C. §3401 (1994). In the context

The consequence of the Court's attempts to apply the *Katz* "reasonable expectation of privacy" doctrine in the cases which led to the doctrines set forth above was to reject Fourth Amendment coverage without questioning whether the Court preserved the meaningful purpose behind the protection of privacy.[84] The Court has a special duty to protect the right of the people to be left alone when the government intrudes upon that right of privacy.[85] However, the Court's failure to recognize its obligation to be sensitive to the risks that citizens assume in a free and open society has led it to ignore the historical purpose of the Amendment. According to the Constitution, the Fourth Amendment was to act as a limitation upon the exercise of governmental power.[86] No part of today's society needs more protection from the exercise of government power than the greatly increasing number of citizens who communicate by sending and receiving electronic mail via the Internet.[87]

## IV. THE INTERNET AND ELECTRONIC MAIL

*Progress imposes not only new possibilities for the future but new restrictions.*[88]

### A. *The Internet*

The Internet originated as a network of computers that began as an experiment of the Defense Department's Advanced Research Project Agency ("ARPA") and was called the Advanced Research Project Agency Network ("ARPANET").[89] The ARPA designed the Internet as a

---

of e-mail, these cases demonstrate that while both parties to a conversation have standing to object to the interception of their conversation, each assumes the risk that the other might reveal the information to the government, depriving the person of standing to exclude the admission of the communication into evidence.

[84] *See supra* notes 18-30 and accompanying text (explaining the history of the Fourth Amendment). *See also* Gutterman, *supra* note 9, at 671 (explaining that "the Court failed to assess the effect that the uncontrolled government activity would have on our daily lives").

[85] *See supra* notes 18-30 and accompanying text (explaining the history of the Fourth Amendment).

[86] *See id. See also* Gutterman *supra* note 9, at 731-32 (describing how the Court has come full circle back to the decision in *Olmstead* because of the Court's bias toward the needs of law enforcement).

[87] *See infra* notes 89-100 and accompanying text (explaining the Internet and electronic mail).

[88] NORBERT WIENER, THE HUMAN USE OF HUMAN BEINGS (1954) (leading mathematician and pioneer in the mathematics of computer theory, who originated the term "cybernetics").

[89] ACLU v. Reno, 929 F. Supp 824, 831 (E.D. Pa 1996). This network linked computers and computer networks owned by the military, defense contractors, and university laboratories conducting defense-related research. *Id.* As ARPANET evolved far beyond

decentralized network of computer networks that formed a single network of redundant links, capable of automatically re-routing communications if a military attack or simple technical malfunction damaged one of the links.[90] One type of communication sent over this redundant series of linked computers was "electronic mail."[91]

### B. *Electronic Mail*

"Electronic mail," more commonly referred to as "e-mail," is a form of private communication in which the sender of an e-mail message uses a keyboard to type a message into a computer and a modem to transmit the message over a telephone line to a recipient via the Internet.[92] The Internet uses a universal protocol, called Simple Mail Transfer Protocol ("SMTP"), to transfer e-mail.[93] However, e-mail messages sent between computers on the Internet do not necessarily travel entirely along the same path.[94]

Most networks that transmit e-mail through the Internet use the "store-and-forward" method.[95] Under the store-and-forward method, the sending computer subdivides a message into smaller "packets" marked with the destination address of the recipient and a code marking the packet's sequence number within the whole message.[96] The sending computer then transmits the smaller "packets" to the nearest

---

its research origins, it became known as "DARPA INTERNET" and finally just the "Internet." *Id.*

[90] *Id.* The ARPA designed the network to be a decentralized, self-maintaining series of redundant links between computers and computer networks, capable of transmitting communications without human control and with the automatic ability to re-route communications if a nuclear war damaged one of the links, so that vital communications could continue. *Id.* The collection of these many different networks use a common protocol called Transmission Control Protocol/Internet Protocol ("TCP/IP") so that all the computers on the network speak the same language despite their main operating system. *See* HARLEY HAHN & RICK STOUT, THE INTERNET COMPLETE REFERENCE 29-30 (1994).

[91] *See infra* notes 92-100 and accompanying text (discussing "electronic mail").

[92] *See* PALME, *supra* note 3, at 4.

[93] *See id.* at 129. Simple Mail Transfer Protocol (SMTP) is part of the TCP/IP family of protocols, which transfer mail from one host computer to another on the Internet. *Id. See also* HAHN & STOUT, *supra* note 90, at 68-69. If e-mail is sent from one network to another network with a different protocol than SMTP, the message has to be routed through a gateway. *See* PALME, *supra* note 3, at 174. Private commercial networks, such as America Online or CompuServe route e-mail through a gateway that converts the e-mail from SMTP format to their proprietary standard or vice versa. *Id.* Nevertheless, the entire process is nearly a seamless process of sending, routing, gatewaying if necessary, and finally receiving. *See id.* at 153-56.

[94] *ACLU*, 929 F. Supp. at 831. *See also* HAHN & STOUT, *supra* note 90, at 30.

[95] *See* PALME, *supra* note 3, at 59-62.

[96] *See* HAHN & STOUT, *supra* note 90, at 30.

intermediate computer called a station.[97] The station further transmits the smaller "packets" to other intermediate stations until all of the packets reach the receiving computer where the "packets" line up in sequence.[98] Then the receiving computer reassembles the "packets" and places the communication into the recipient's e-mail mailbox account.[99] While all "packets" of a particular message sometimes travel along the same path to the destination address, if one of the stations along the route becomes congested, then some of the "packets" can be re-routed along the path of least resistance to less congested stations.[100] In order to protect the privacy of these "packets," Congress enacted legislation that attempted to balance Fourth Amendment protections with emerging technologies.[101]

---

[97] *See* PALME, *supra* note 3, at 60.
[98] *See* HAHN & STOUT, *supra* note 90, at 30.
[99] *Id.*
[100] *Id.*
[101] *See infra* notes 103-227 and accompanying text (discussing the Electronic Communications Privacy Act).

## V. THE PRIVACY OF ELECTRONIC COMMUNICATIONS

*Gentlemen [and ladies] do not read each other's mail.*[102]

Congress enacted the Federal Wiretap Act in Title III of the Omnibus Crime Control and Safe Streets Act of 1968[103] in response to the Supreme Court's decisions in *Katz* and *Berger*.[104] Because Congress worried that newly developed means of eavesdropping posed a serious threat to privacy rights, the Act aimed to protect the privacy rights of "wire" and "oral" communication by prohibiting private interception.[105] Likewise, the Act provided strict guidelines for government interception.[106]

In 1986, Congress broadened the Act to include an "electronic communication"[107] and renamed it the Electronic Communications Privacy Act ("ECPA").[108] The ECPA consists of Title I and Title II as codified in chapters 119[109] and 121,[110] respectively, of Title 18 (Crimes and Criminal Procedure) of the United States Code ("U.S.C."). In this section, this Note examines what protection Title I and Title II provide an "electronic communication," when the protection applies, and what protection Title I and Title II do not provide.

---

[102] HENRY L. STIMSON, ON ACTIVE SERVICE IN PEACE AND WAR 7 (1948).

[103] Pub. L. No. 90-351, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2520 (1994)).

[104] *See supra* note 55-64 and accompanying text (discussing the *Katz* decision of 1967). Also in 1967, the Court decided Berger v. New York, 388 U.S. 41 (1967). In *Berger*, the Court held that any form of electronic surveillance, including wiretapping, must satisfy certain requirements: the warrant must describe with particularity the conversations to be overheard, show probable cause that a specific crime has been or is being committed, limit the time period for the surveillance, name the suspects to be overheard, require a return to the court to show what conversations were intercepted, and must terminate when the government obtains the desired information. *Id.* at 59-60. *See also* S. REP. NO. 90-1097, at 10 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153 (explaining that Congress passed the act to satisfy *Berger* and *Katz*).

[105] *See* 18 U.S.C. § 2511 (1) (1994).

[106] *See* 18 U.S.C. § 2518 (1994).

[107] The ECPA encompasses many formerly unprotected modes of communication by redefining the term "electronic communication." *See infra* note 113 (defining "electronic communication").

[108] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C.). *See* 18 U.S.C. §§ 2510-2522, 2701-2711, 3117, 3121-3127 (1994). This Note argues that with Fourth Amendment protection in doubt because of the Court's lack of focus on the true *Katz* standard, the ECPA must be reworked to give private e-mail the true protection that the Fourth Amendment intended to give all private communications.

[109] For chapter 119 (Wire and Electronic Communications Interception and Interception of Oral Communications), see 18 U.S.C. § 2511 (1994).

[110] For chapter 121 (Stored Wire and Electronic Communications and Transactional Records Access), see 18 U.S.C. § 2701 (1994). *See also* EDWARD A. CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW 168 (1996).

### A. Title I: The Interception and Disclosure of Electronic Communications

Title I of the ECPA proscribes the unauthorized interception of "wire,"[111] "oral,"[112] or "electronic"[113] communication and the use or disclosure of an intercepted "wire," "oral," or "electronic" communication.[114] In regard to an e-mail communication, any government employee who commits either of the following two actions without a court order violates the ECPA.[115] First, a person[116] acts in violation of the ECPA if that person intentionally "intercepts" or endeavors to "intercept" any "electronic communication" while in transmission.[117] Second, a person acts in violation of the ECPA if that person intentionally uses or discloses or endeavors to use or disclose the "contents"[118] of any "electronic communication" while knowing or having reason to know that the information was obtained through the

---

[111] Section 2510 (1) defines "wire communication" as:

> any aural transfer in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or 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 in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication.

18 U.S.C. § 2510(1) (1994).

[112] Section 2510(2) defines "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, but such term does not include any electronic communication." 18 U.S.C. § 2510(2) (1994).

[113] Section 2510(12) defines "electronic communication" as:

> any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—(a) any wire or oral communication; (b) any communication made through a tone-only paging device; (c) any communication from a tracking device (as defined in section 3117 of this title); or (d) electronic funds transfer information stored by a financial institution in a communications system used for electronic storage and transfer of funds.

18 U.S.C. § 2510(12) (1994).

[114] 18 U.S.C. § 2511 (1994).

[115] *See infra* notes 116-20 and accompanying text. *See also* CAVAZOS & MORIN, *supra* note 110, at 17.

[116] 18 U.S.C. § 2510 (6). Section 2510 (6) defines a "person" as "any employee, or agent of the United States or any State or of a State of political subdivision thereof . . . ." *Id.*

[117] *See* 18 U.S.C. § 2511 (1) (a)-(b) (1994).

[118] Section 2510 (8) defines "contents" as "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (1994).

interception of an "electronic communication."[119] Both of these violations can only occur after an unauthorized interception.[120]

While the ECPA makes it illegal for any person, including a system operator, to intercept or disclose an e-mail communication to anyone other than the addressee or intended recipient of such communication,[121] the Act does not prohibit a system operator from disclosing the contents of a communication to a law enforcement agency in any of four situations. First, a system operator may divulge the contents of a communication if authorized under section 2511(2)(a) or 2517.[122] Second, a system operator may divulge the contents of a communication with the lawful consent of either the sender or the intended recipient of such communication.[123] Third, a system operator may divulge the contents of a communication to whomever it is necessary to forward the communication to its destination.[124] Lastly, a system operator may divulge the "contents" of an inadvertently obtained communication that appears to pertain to the commission of a crime, but only to a law enforcement agency.[125]

When the government conducts an authorized interception or surveillance on a particular system, the ECPA places restrictions on a system operator.[126] No provider of an "electronic communication

---

[119] *See* 18 U.S.C. § 2511(1)(c)-(d) (1994).

[120] Section 2510 (4) defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (1994).

[121] Section 2511(3)(a) states that "an electronic communication service to the public shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication . . . ." 18 U.S.C. § 2511(3)(a) (1994).

[122] 18 U.S.C. § 2511(3)(b)(i) (1994). Section 2511 (2) (a) is overly broad because by its terms it allows:

> a provider of . . . electronic communication service . . . to intercept, disclose, or use that communication in the normal course of his employment while engaged in *any activity* which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except . . . random monitoring . . . [done other than] for . . . quality control checks.

18 U.S.C. § 2511(2)(a)(i) (1994) (emphasis added). *See also* section 2517, "Authorization for disclosure and use of intercepted wire, oral, or electronic communications." 18 U.S.C. § 2517 (1994).

[123] 18 U.S.C. § 2511(3)(b)(ii) (1994).

[124] 18 U.S.C. § 2511(3)(b)(iii) (1994).

[125] 18 U.S.C. § 2511(3)(b)(iv); *see also supra* note 122 and accompanying text (explaining that section 2511(3)(b)(i) is overly broad and allows system operators too much discretion).

[126] *See* 18 U.S.C. § 2511(2)(a)(ii)(B) (1994).

service"[127] or any of its employees can disclose the existence of any interception, surveillance, or disclose the device used to accomplish the interception or surveillance, unless required to by the legal process.[128] In addition, authorized disclosure may occur only after prior notification to the Attorney General or to the principal prosecuting attorney.[129] Any unauthorized disclosure renders the "electronic communication service" or particular employee liable for civil damages.[130]

The ECPA also permits any government attorney or state law enforcement officer to make an application for a pen register[131] or trap and trace device[132] to a court of competent jurisdiction.[133] Upon application, the court can enter an *ex parte* order authorizing the installation and use of either device, if the information sought is relevant to an ongoing criminal investigation.[134] As with other parts of the ECPA, these provisions indicate a congressional codification of the Court's prior holding in cases interpreting the Fourth Amendment.[135] For example, a person can lawfully "intercept" an "electronic communication," when such person is a party to the communication or when one of the parties to the communication gave prior consent to such interception.[136] In addition, a person can lawfully "intercept" or access an "electronic communication" made through an "electronic communication system"[137]

---

[127] Section 2510(15) defines an "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (1994).

[128] *Id.*

[129] *Id.*

[130] *Id.* For recovery of civil damages, *see* 18 U.S.C. § 2520 (1994).

[131] Section 3127(3) defines a "pen register" as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached . . . ." 18 U.S.C § 3127(3) (1994).

[132] Section 3127(4) defines a "trap and trace device" as "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 18 U.S.C. § 3127(4) (1994).

[133] Section 2511(2) (h) makes it lawful "to use a pen register or a trap and trace device . . . ." 18 U.S.C. § 2511(2)(h) (1994). For the application guidelines for the order of a pen register or a trap and trace device, see 18 U.S.C. § 3122 (a)-(b) (1994).

[134] *See* 18 U.S.C. § 3123(a) (1994).

[135] *See* Smith v. Maryland, 442 U.S. 735, 742-44 (1979) (holding that because a defendant has no reasonable expectation of privacy that the telephone company will not disclose the telephone numbers he dials to the police, the use of pen registers to record the numbers dialed from a particular phone is not a search). *See also supra* notes 81-83 and accompanying text (explaining the "assumption of the risk" doctrine).

[136] 18 U.S.C. § 2511(2)(c) (1994). *See also supra* notes 68-74 and accompanying text (explaining the "standing" doctrine).

[137] Section 2510(14) defines an "electronic communication system" as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic

that is configured so that such communication is readily accessible to the general public.[138]

Although the ECPA protects e-mail and other forms of "electronic communication" from private interception, the law fails to afford "electronic communication" the same protection from government interception that a "wire" or "oral" communication receives.[139] First, an "electronic communication" may be intercepted for any federal felony whereas a "wire" or "oral" communication may be intercepted for only a handful of enumerated offenses.[140] Second, an application to a federal judge for a court "intercept" order to obtain an "electronic communication" may be approved by the Attorney General, any U.S. Attorney, or any authorized Assistant Attorney General or Assistant U.S. Attorney.[141] In contrast, an application to a federal judge for a court "intercept" order to obtain a "wire" or "oral" communication may only be approved by specifically designated attorneys in the Criminal Division of the U.S. Attorney's Office located in Washington, D.C.[142] Third, an "electronic communication" may be suppressed only through the judicially created "exclusionary rule" when a constitutional violation occurs,[143] whereas a "wire" or "oral" communication may be suppressed

---

communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510 14) (1994).

[138] 18 U.S.C. § 2511(2)(g)(i) (1994). *See also supra* notes 81-83 and accompanying text (explaining the "assumption of the risk" doctrine).

[139] *See infra* notes 140-45 and accompanying text. *See also* Michael S. Leib, *E-mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception*, 34 HARV. J. ON LEGIS. 393, 406-09 (1997).

[140] *See* 18 U.S.C. § 2516(1994). Section 2516 (3) states that "any attorney for the Government (as such term is defined for purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge . . . for . . . an order authorizing . . . the interception of electronic communications when such interception may provide or has provided evidence of any Federal felony." 18 U.S.C. § 2516(3). Moreover, the Federal Rule of Criminal Procedure defines a "government attorney" as the "Attorney General, any U.S. Attorney, or any authorized Assistant Attorney General or Assistant U.S. Attorney." Fed. R. Crim. P. 54 (c). In comparison, section 2516(1)(a), (b), and (c) state that specifically designated attorneys in the Criminal Division located in Washington, D.C., "may authorize an application to a Federal judge . . . for, . . . an order authorizing . . . the interception of wire or oral communications . . . when such interception may provide or has provided evidence of" a list of crimes such as the sabotage of nuclear facilities, treason, espionage, murder, kidnapping, or Presidential assassination. 18 U.S.C. § 2516(1)(a), (b), (c) (1994).

[141] *See supra* note 140.

[142] *Id.*

[143] *See supra* notes 27-30 and accompanying text (explaining how the "exclusionary rule" forbids the admission of evidence obtained in violation of the Fourth Amendment). *See also supra* notes 55-83 and accompanying text (discussing what constitutes a violation of

through the statutorily created "exclusionary rule" whenever the violation of a "central"[144] provision of the ECPA occurs.[145] These three distinctions pose a serious threat to the use of new technologies, because citizens will forgo the use of new technologies in favor of older technologies that provide more privacy protection from government interception.[146] However, fear of government interception poses only half of the problem. An even greater threat to the privacy of e-mail communications is government access to a stored "electronic communication."[147]

---

the Fourth Amendment). If a person or the government illegally intercepts an "electronic communication," but commits no constitutional violation, then the only remedies or sanctions available against the person or government are criminal or civil in nature, under section 2511(4)(a) and section 2520. *See* 18 U.S.C. §§ 2511(4)(a), 2520 (1994). Moreover, section 2518(10)(c) reads that "[t]he remedies and sanctions described in this chapter [18 U.S.C. 2511(4)(a) and 2520] with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations . . . ." 18 U.S.C. § 2518(10)(c).

[144] *See* United States v. Chavez, 416 U.S. 562, 578 (1974) (holding that only an error in an application that affects a "central" or "functional" provision of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 will trigger the statutory suppression remedy).

[145] Section 2515 states that:

> Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

18 U.S.C. § 2515 (1994). In addition, section 2518 states that:

> Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, 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 . . . .

18 U.S.C. § 2518 (10)(a).

[146] The framers of the Constitution founded the United States on the basis that a free society requires that each citizen have the ability to communicate freely, openly, and privately without fear of government eavesdropping. *See* U.S. CONST. amend. I.

[147] *See infra* notes 148-227 and accompanying text.

### B. *Title II: The Access to and Disclosure of Stored Wire and Electronic Communications*

Title II of the ECPA proscribes most access to and disclosure of a stored "wire" or "electronic communication."[148] In regard to the unauthorized "access" of a stored private e-mail communication, the ECPA has a dual purpose.[149] First, the ECPA outlaws most unauthorized private access.[150] Second, the ECPA provides prerequisites for government access.[151] A government entity may require an "electronic communication service" to disclose the contents of an "electronic communication" held in "electronic storage" for 180 days or less only pursuant to a warrant supported by probable cause.[152] In comparison, a government entity may require an "electronic communication service" to disclose the contents of an "electronic communication" held in "electronic storage" for more than 180 days pursuant to a warrant, administrative subpoena, or court order.[153] Unlike a warrant supported by probable cause, an administrative subpoena requires no factual basis and a court order requires a mere offering of "specific and articulable" facts showing reasonable grounds to believe that the contents of an "electronic communication" are relevant to an ongoing criminal investigation.[154] Thus, the ECPA provides less protection for an "electronic communication" held in "electronic storage," especially when compared to a "wire communication" held in "electronic storage."[155]

---

[148] 18 U.S.C §§ 2701-11 (1994). The victim of an unauthorized access or improper disclosure of a private "electronic communication" has a civil cause of action. 18 U.S.C. § 2707 (1994).

[149] *See infra* notes 150-51 and accompanying text.

[150] Section 2701(a)(1) makes it unlawful to "intentionally access without authorization a facility through which an electronic communication service is provided." 18 U.S.C. § 2701(a)(1) (1994). In addition, section 2701(a)(2) makes it unlawful to "intentionally exceed[] an authorization to access that facility; and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage . . . ." 18 U.S.C. § 2701(a)(2) (1994). A person who violates section 2701(a) may suffer penalties. *See* 18 U.S.C. § 2701(b) (1994). However, section 2701(c) provides exceptions. *See* 18 U.S.C. § 2701(c) (1994). In particular, section 2701(c)(3) provides exceptions with respect to government conduct authorized in section 2703, 2704, or 2518. 18 U.S.C. § 2701(3) (1994). *See infra* notes 151-53 and accompanying text (explaining the exception for government conduct in section 2703).

[151] *See* 18 U.S.C. § 2703(a) (1994).

[152] 18 U.S.C. § 2703(a).

[153] 18 U.S.C. § 2703(a)-(d).

[154] 18 U.S.C. § 2704(d).

[155] *See infra* notes 156-58 and accompanying text (explaining that an "electronic communication" held in "electronic storage" does not receive the same protection as a "wire communication" held in "electronic storage").

Although the ECPA provides some protection for e-mail and other forms of "electronic communication" held in "electronic storage," the law does not provide an "electronic communication" the same level of protection from government access that a "wire communication" receives.[156] Government access to a stored "wire communication" requires an intercept order,[157] whereas the government can access a stored "electronic communication" through a warrant, subpoena, or court order.[158] In other words, a stored "wire communication" receives the strict protection found in the Title I court "intercept" order, whereas an "electronic communication" receives the less stringent protection found in Title II.[159]

In regard to the "disclosure" of a stored "electronic communication" in the form of a private e-mail, the ECPA proscribes a person or entity providing an "electronic communication service" to the public from knowingly divulging to anyone the "contents" of a communication while in "electronic storage."[160] However, an "electronic communication service" may divulge the "contents" to an addressee or intended recipient of such communication[161] or to a person whose facilities are used to forward a communication to its intended destination.[162] Likewise, an "electronic communication service" may divulge the contents of an "electronic communication" that may be necessarily incident to the rendition of that service, such as to protect the property of the service[163] or as otherwise authorized in other sections of the ECPA.[164] Lastly, if the "electronic communication service" inadvertently obtains the contents of an "electronic communication" that appear to pertain to

---

[156] *See* 18 U.S.C. §§ 2701-2711.

[157] *See* 18 U.S.C. §§ 2516, 2218 (1994).

[158] *See supra* notes 150-53 and accompanying text.

[159] The distinction lies in the definitions of a "wire communication" and an "electronic communication." The definition of a "wire communication" . . . "includes any storage of such communication," implying that the access to a stored "wire communication" remains protected under Title I. 18 U.S.C. § 2510(1) (1994). In comparison, the definition of an "electronic communication" does not include any storage of such communication. *See* 18 U.S.C. § 2510 (12). For the definition of an "electronic communication," see *supra* note 113. The storage of an "electronic communication" is not included in section 2510(12) because access to a stored "electronic communication" is protected under Title II. *See* 18 U.S.C. § 2701 (1994).

[160] 18 U.S.C. § 2702 (1994).

[161] 18 U.S.C. § 2702(b)(1) ("or an agent of such addressee or intended recipient").

[162] 18 U.S.C. § 2702(b)(4) ("to a person employed or authorized or whose facilities are used to forward such communication to its destination").

[163] 18 U.S.C. § 2702(b)(5) ("as may be necessarily incident to the rendition of such service or to the protection of the rights or property of the provider of that service").

[164] 18 U.S.C. § 2702(b)(2) ("as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title").

the commission of a crime, then the service provider may divulge the contents to the government.[165]

A court first interpreted the ECPA in *Steve Jackson Games v. United States Secret Service*,[166] a case involving a stored "electronic communication" in the form of a private e-mail. In an early morning raid on March 1, 1990, the Secret Service searched the offices of Steve Jackson Games, Inc. ("SJG"), a role-playing games publisher.[167] The Secret Service suspected that SJG was a haven to the "Legion of Doom" ("LOD"), a loose association of notorious hackers[168] who apparently stole a sensitive and proprietary document detailing the operation of Bell South's Emergency 911 ("E911") telephone system.[169] Hence, the Secret Service obtained a warrant to search SJG.[170] But soon after the Secret

---

[165] 18 U.S.C. § 2702(b)(6).

[166] 816 F. Supp. 432 (W.D. Tex. 1993).

[167] *Id.* at 437. SJG publishes books, magazines, box games, and related products. *Id.* at 434. In addition, SJG operates an electronic bulletin board system ("BBS") called "Illuminati," named after one of the company's most successful products. *Id.* The BBS:

> posts information to the inquiring public about Steve Jackson Games' products and activities; provides a medium for receiving and passing on information from the corporation's employees, writers, customers, and its game enthusiasts; and finally, affords its users electronic mail whereby, with the use of selected passwords, its users can send and receive private e-mail . . . .

*Id.*

[168] *See* CAVAZOS & MORIN, *supra* note 110, at 22. A "hacker" is an individual who accesses a computer system without authority. *Steve Jackson Games*, 816 F. Supp. at 435 n.2.

[169] *Steve Jackson Games*, 816 F. Supp. at 436.

[170] The search warrant authorized the seizure of:

> Computer hardware (including, but not limited to, central processing unit(s), monitors, memory devices, modem(s), programming equipment, communication equipment, disks, and prints) and computer software (including, but not limited to, memory disks, floppy disks, storage media) and written material and documents relating to the use of the computer system (including networking access files), documentation relating to the attacking of computers and advertising the results of computer attack (including telephone numbers and licensing documentation relative to the computer programs and equipment at the business known as Steve Jackson Games which constitute evidence, instrumentalities and fruits of federal crimes, including interstate transportation of stolen property (18 USC 2314) and interstate transportation of computer access information (18 USC 1030 (a)(6)). This warrant is for the seizure of the above described computer and computer data and for the authorization to read information stored and contained on the above described computer and computer data.

Jim Thomas & Gordon Meyer, Secret Service Search Warrant Affidavit, 2 COMPUTER UNDERGROUND DIGEST 2.11 (November 13, 1990)

Service executed the search warrant, the Agency learned that the connection between SJG and the LOD or the E911 document was erroneous.[171] While one of SJG's employees, a co-systems operator,[172] claimed membership in the LOD and was writing a fantasy role-playing game about computer hacking, not a scintilla of evidence indicated illegal activity at the company.[173] The Secret Service made a mistake and erroneously believed that the Agency harbored substantial criminal information.[174] But the evidence was obviously insufficient as the Secret Service neither arrested nor filed any criminal charges against any member of SJG, including the co-systems operator.[175]

Nevertheless, during the raid of SJG, the Secret Service seized three computers, primarily targeting the computer used for the company's bulletin board system ("BBS").[176] The BBS stored private e-mail on the computer's hard disk drive temporarily until the addressees used their computers and modems to remotely access the BBS and receive their e-mail.[177] After receiving and reading their e-mail, the recipients chose to either delete the e-mail permanently or to store the e-mail on the BBS computer's hard disk drive.[178]

At the time of the raid, the Secret Service seized 162 items of unread, private e-mail[179] from some of the 365 BBS users.[180] Consequently, the intended recipients of the unread, private e-mail, along with Steve

---

http://www.sjgames.com/SS/affidavit.html; Brief for Appellant at Record Excerpts, Attachment B.

171 CAVAZOS & MORIN, *supra* note 110, at 23.

172 *Steve Jackson Games*, 36 F.3d 457, 459 (5th Cir. 1994) (explaining that Loyd Blankeship was a co-systems operator of the Bulletin Board System ("BBS") and had the ability to review and delete any data on the BBS).

173 The court proclaimed:

> Importantly, prior to March 1, 1990 (the date that the Secret Service raided SJG), and at all other times, there has never been any basis for suspicion that any of the Plaintiffs [SJG, Steve Jackson, Elizabeth McCoy, Walter Milliken, or Steffan O'Sullivan] have engaged in any criminal activity, violated any law, or attempted to communicate, publish, or store any illegally obtained information or otherwise provide access to any illegally obtained information or to solicit any information which was to be used illegally.

*Steve Jackson Games*, 816 F. Supp. at 435.

174 *Id.* at 437.

175 *Id.*

176 *Id.* During the search of SJG, the Secret Service seized three computers, over 300 computer disks, and other materials. *Id.*

177 *Steve Jackson Games*, 36 F.3d at 458.

178 *Id.*

179 *Id.* at 459.

180 *Id.*

Jackson and his company, sued the Secret Service because it opened, read, and deleted their private e-mail.[181] In other words, the plaintiffs claimed that by seizing the BBS and accessing their private e-mail stored on its hard disk drive, the Secret Service illegally intercepted and disclosed private communications in violation of both Title I[182] and Title II[183] of the ECPA.[184]

After reviewing Title I and Title II, the district court held that the Secret Service did not "intercept" the plaintiffs' e-mail in violation of Title I[185] because the Secret Service did not acquire the e-mail contemporaneously with its transmission.[186] But the district court also held that the Secret Service did disclose and use, without authorization, all of the private e-mail stored on the BBS in violation of Title II.[187] Because the Secret Service violated Title II of the ECPA, the district court

---

[181] *Steve Jackson Games*, 816 F. Supp. at 438. While the Secret Service denied that the Agency's personnel read the private e-mail and specifically alleged that the Agency only used a key word search to review the e-mail, the court found that the preponderance of the evidence, including common sense, established that the Secret Service did read all of the e-mail seized and did delete certain information. *Id.* In fact, the court noted that the Secret Service worded the search warrant so that all information would be "read." *Id.* at 438 n.5. *See also supra* note 170 for the text of the search warrant.

[182] For a thorough discussion of Title I of the ECPA §§ 2510-2521, see *supra* notes 111-46.

[183] For a thorough discussion of Title II of the ECPA §§ 2701-2711, see *supra* notes 148-227.

[184] *Steve Jackson Games*, 816 F. Supp. at 434. The plaintiff's lawsuit also stated a cause of action pursuant to the Privacy Protection Act, 42 U.S.C. 2000aa. *Id.* But that claim is outside the scope of this Note and will not be addressed.

[185] *Steve Jackson Games*, 816 F. Supp. at 432 (declining to find liability for any plaintiff pursuant to the Title I).

[186] The district court relied on *United States v. Turk*, a Fifth Circuit Court of Appeals case interpreting "intercept" under Title III of the Federal Wiretap Act of 1968. United States v. Turk, 526 F.2d 654 (5th Cir.), *cert. denied*, 429 U.S. 823 (1976). In *Turk*, law enforcement officers who arrested two men for transporting cocaine and firearms, seized, and played two cassette tapes without obtaining a warrant. *Id.* at 656. Subsequently, the government used the information taken from these recordings to convict the defendant of perjury. *Id.* at 657. As a defense, the defendant claimed that the officers illegally intercepted the private communication under the Federal Wiretap Act. *Id.* The *Turk* court analyzed the definition of "intercept" under the Act and concluded "that an 'intercept' requires, at the least, involvement in the initial use of the device contemporaneous with the communication to transmit or preserve the communication." *Turk*, 526 F.2d at 658 n.3. In other words, the *Turk* court concluded that an "intercept" "require[s] participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of the device." *Id.* at 658.

[187] *Steve Jackson Games*, 816 F. Supp. at 443 (finding that the Secret Service exceeded its authority under Title II); *see also Steve Jackson Games*, 36 F.3d at 459 (explaining that the Secret Service violated Title II when it seized stored e-mail without complying with the statutory provisions).

awarded each individual plaintiff $1,000 in statutory damages[188] along with attorneys' fees and court costs in bringing the suit.[189] However, the statutory damage award under Title II did not satisfy the plaintiffs, and they appealed to the Court of Appeals for the Fifth Circuit.[190] In the court of appeals, the plaintiffs claimed that the Secret Service illegally intercepted their private e-mail in violation of Title I[191] and that Title I entitled them to a $10,000 statutory damage award.[192]

The Court of Appeals for the Fifth Circuit addressed the narrow issue of whether the seizure of the BBS which contained private e-mail that had been sent, but not yet received (read) by the recipients, constituted an "intercept" proscribed by Title I.[193] To decide the issue, the court of appeals analyzed many of the ECPA's technical terms defined in section 2510.[194] First, the court of appeals examined the definition of an "electronic communication,"[195] an "intercept,"[196] an "aural transfer,"[197] and "electronic storage."[198] Second, the court of appeals noted that, unlike the definition of a "wire communication" which includes any "electronic storage" of such communication, the definition of an "electronic communication" does not include the

---

[188] *Steve Jackson Games*, 816 F. Supp. at 443. Title II awards statutory damages in section 2707(c) which states that "[t]he court may assess as damages . . . under this section the sum of the actual damages suffered by the plaintiff . . . but in no case shall a person entitled to recover receive less than the sum of $1,000." 18 U.S.C. § 2707(c) (1994).

[189] *Steve Jackson Games*, 816 F. Supp. at 444.

[190] *Steve Jackson Games*, 36 F.3d at 457.

[191] The sole issue before the court of appeals was whether the seizure of a computer, used to operate a BBS, containing private e-mail which had been sent to (stored on) the BBS, but not read (received) by the intended recipients, constituted an unlawful intercept under Title I. *Id.* at 458.

[192] Title I awards statutory damages in section 2520(c)(2)(B) which states that "[t]he court may assess as statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000." 18 U.S.C. § 2520(c)(2)(B) (1994).

[193] *Steve Jackson Games*, 36 F.3d at 458. The court of appeals narrowed the issue by stating that the issue is not whether e-mail can be "intercepted," because it can. *Id.* at 461. Instead, at issue was what constitutes an illegal "intercept." *Id.*

[194] *Id.* at 460-62.

[195] *See supra* note 113 for the definition of an "electronic communication."

[196] *See supra* note 120 for the definition of an "intercept."

[197] Section 2510(18) defines "aural transfer" as "a transfer containing the human voice at any point between and including the point of origin and the point of reception." 18 U.S.C. § 2510(18) (1994).

[198] Section 2510(17) defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510 (17) (1994).

"electronic storage" of such communication.[199] This distinction, the court of appeals added, was critical to determining what constituted an interception.[200] The court of appeals reasoned that Congress used the word "transfer" in the definition of "electronic communication" and omitted any "electronic storage" of such communication because it did not intend for "intercept" to apply to an "electronic communication" held in "electronic storage."[201] Thus, the court of appeals concluded that the Secret Service seizure of the BBS, which contained the private, unread e-mail, was not an illegal interception because the communications were in storage.[202] In other words, the Secret Service did not violate Title I of the ECPA, but it did violate Title II of the ECPA.[203]

The Court of Appeals for the Fifth Circuit reached its holding by determining the legislative intent through the plain language of the ECPA, corroborating its decision by analyzing the ECPA's legislative history.[204] First, the court of appeals noted, as did the district court, that the Senate Report accompanying the ECPA indicated that Congress did not intend to change the definition of "intercept."[205] Second, the court of appeals relied on the fundamental rule that when construing a statute the court should not confine its interpretation to the one portion at issue.[206] Rather, the court should consider the whole statute.[207] Thus, the

---

[199] *Steve Jackson Games*, 36 F.3d at 461. *See also* United States v. Reyes, 922 F. Supp. 818, 836 (1996) (following this definitional interpretation).

[200] *Steve Jackson Games*, 36 F.3d at 461.

[201] *Id.* at 461-62. A stored "wire communication" is subject to different treatment than a stored "electronic communication." *Id.* at 461 n.7. Generally, a search warrant, rather than a court order, is required to obtain access to the "contents" of a stored "electronic communication." 18 U.S.C. § 2703(a) (1994). In contrast, compliance with the more stringent court "intercept" order in section 2518 is required to obtain access to a stored "wire communication" because section 2703 clearly applies only to a stored "electronic communication," not to a stored "wire communication." 18 U.S.C. § 2703 (1994); *see also* H.R. REP. NO. 99-647, at 67-68 (1986).

[202] *Steve Jackson Games*, 36 F.3d at 461-62.

[203] *Id.* at 462.

[204] *Id.* The court of appeals noted that while the goal of statutory construction is to ascertain legislative intent through the plain language of a statute, "when interpreting a statute as complex as the Wiretap Act, which is famous (if not infamous) for its lack of clarity, . . . it [is] appropriate to note the legislative history for confirmation of . . . Congress' intent." *Id.*

[205] *Steve Jackson Games*, 36 F.3d at 462. The Senate Report explains that "[s]ection 101 (a) (3) of the ECPA amends the definition of the term "intercept" . . . to cover electronic communications. . . . The definition of "intercept" under current law is retained . . . except that the term "or other" is inserted after "aural." *Id.* (quoting S. REP NO. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567).

[206] *Id.*

[207] *Id.*

court of appeals concluded that neither the ECPA nor its legislative history indicated that Congress intended for conduct punishable under Title II to also be punishable under Title I.[208]

The Court of Appeals for the Fifth Circuit explained that the distinctions between the Titles persuasively indicated that Congress did not intend for conduct clearly prohibited under Title II to furnish the basis for a civil remedy under Title I.[209] First, the requirements for authorization to "intercept" an "electronic communication" under Title I are substantively different from the requirements for accessing the "contents" of a stored "electronic communication" under Title II.[210] Unlike Title II, which only requires the government to obtain a search warrant to access a stored "electronic communication,"[211] Title I requires that the government procure a court "intercept" order to obtain an "electronic communication" in transit.[212] Second, a court "intercept" order authorizing the seizure of an "electronic communication" under Title I directs the government to comply with additional procedural requirements that a search warrant authorizing access to a stored "electronic communication" under Title II does not impose.[213] Unlike a search warrant under Title II, a court "intercept" order under Title I

---

[208] *Id.* at 462-63.

[209] *Steve Jackson Games*, 36 F.3d at 462-63.

[210] *Id.*

[211] *See* 18 U.S.C. § 2703(a) (1994).

[212] *See* 18 U.S.C. § 2518(1)-(2) (1994). A "judge of competent jurisdiction" may approve an application to intercept a wire, oral, or electronic communication if the application includes: (a) the name of the officer making the application; (b) a full and complete statement of the facts which justify his belief that an order should be issued, including (i) details as to the particular offense, (ii) the nature and location of the facilities where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person who committed the offense, if known; (c) a statement as to whether or not other investigative procedures have been tried and failed; (d) a statement about the period of time for which the interception is required; (e) a statement of facts about all previous applications for the same individual; and (f) if the application is for the extension of an order, a statement setting forth the results obtained to date. *See* 18 U.S.C. § 2518(1)(a)-(f) (1994). In addition, the "judge of competent jurisdiction" has the authority to require the applicant to furnish additional evidence in support of the application. *See* 18 U.S.C. § 2518(2) (1994). Section 2510(9) defines a "judge of competent jurisdiction" as:

> (a) a judge of a United States district court or a United States court of appeals; and (b) a judge of any court of general jurisdiction of a State court of appeals who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications.

18 U.S.C. § 2510(9) (1994).

[213] *Steve Jackson Games*, 36 F.3d at 463.

includes four additional directives.[214] First, the court order must not be for any period longer than is necessary.[215] Second, the court order must be executed as soon as practicable.[216] Third, the court order must be conducted in a way that minimizes the interception of communications not otherwise subject to interception.[217] Fourth, the court order must pertain to the investigation of an offense enumerated in section 2516.[218] In light of these significant differences in substantive and procedural requirements, the court of appeals concluded that Congress did not intend for conduct punishable under Title II to also be punishable under Title I.[219]

Ultimately, the Court of Appeals for the Fifth Circuit affirmed the district court's reliance on the *Turk*[220] definition of "intercept," as originally applied to a "wire communication," and merely extended it to include an "electronic communication."[221] Thus, the interception of an "electronic communication" requires that the law enforcement agency participate in the contemporaneous acquisition of the communication through the use of a device.[222] However, as anyone familiar with e-mail can attest, this definition of "intercept" poses some serious problems for

---

[214] *See infra* notes 215-18 and accompanying text.

[215] 18 U.S.C. § 2518(5) (1994). Section 2518(5) directs that "[n]o order . . . may authorize . . . for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days." *Id.*

[216] *Id.* Section 2518(5) directs that "[e]very order . . . shall contain a provision that the authorization to intercept shall be executed as soon as practicable." *Id.*

[217] *Id.* Section 2518 (5) directs that "[e]very order . . . shall be conducted in such a way as to minimize the interception of the communications not otherwise subject to interception under this chapter." *Id.*

[218] 18 U.S.C. § 2516 (1994).

[219] *Steve Jackson Games*, 36 F.3d at 463. To further reinforce the court of appeal's holding that Congress intended to draw distinctions between communications in "transit" and communications in "electronic storage," the court emphasized the ECPA legislative history's explanation about the prohibition of disclosure in section 2702(a) of Title II and in section 2511(3) of Title I. *Id.* at 463 n. 8 (citing S. REP. NO. 99-541, 97th Cong. 2nd Sess. 37, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3591). Section 2702(a) of Title II (chapter 121) prohibits "an electronic communication service to the public . . . [from] divulging . . . the contents of a communication while it is in electronic storage." 18 U.S.C. § 2702 (1994). In comparison, section 2511(3) of Title I (chapter 119) prohibits "an electronic communications service to the public . . . from divulging the contents of a communication . . . while in transmission." 18 U.S.C. § 2511(3).

[220] *See supra* note 186 (explaining that the *Turk* decision relied upon by the district court).

[221] Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994), *aff'g* 816 F. Supp. 432, 441-43 (W.D. Tex. 1993) (analogizing that the seizure of an "electronic communication" that had been sent, but not yet received by its addressee was the same as the seizure of a tape recording).

[222] *Steve Jackson Games*, 816 F. Supp. at 441-42.

a citizen's right to privacy.[223] For example, the *Turk* definition of intercept effectively renders the distinction between the authorized interception of an "electronic communication" under Title I and the authorized access to a stored "electronic communication" under Title II meaningless.[224] No law enforcement agency need comply with the more stringent substantive and procedural requirements necessary for a court "intercept" order under Title I[225] when the agency can merely wait to access the desired "electronic communication" held in "electronic storage" with a warrant under Title II.[226] Thus, because a law enforcement agency can wait until an "electronic communication service" holds an "electronic communication" in "electronic storage" and then gain access without a court "intercept" order, Congress must reexamine the ECPA.[227] The following proposed modifications to the ECPA seek to give an "electronic communication" the same level of protection that a "wire" or "oral" communication receives.[228]

## VI. MODIFYING THE ECPA

*Change is the law of life. And those who look only to the past or the present are certain to miss the future.*[229]

When the framers of the Constitution acted to guard against the arbitrary use of government power to maintain surveillance over citizens, only limited methods existed to intrude into those citizens' "houses, papers, and effects."[230] During the intervening 200 years, development of new methods of communication and devices for

---

[223] *See* CAVAZOS & MORIN, *supra* note 110, at 25 (arguing that a tape recorded conversation is a completed communication, but an undelivered e-mail is more like a wiretap because it is seized before it is completed).

[224] For a chart diagramming how the *Turk* definition of "intercept" limits the interception of an electronic communication to situations where the government monitors keystrokes, taps a data line, or reroutes an e-mail to provide contemporaneous acquisition, see CAVAZOS & MORIN, *supra* note 110, at 23 fig.2.1.

[225] *See supra* notes 210-18 and accompanying text (explaining the different substantive and procedural requirements).

[226] *See* 18 U.S.C. § 2703(a) (1994) (explaining the prerequisites for access to stored communications).

[227] The *Steve Jackson Games* decision illustrates the problem with merely extending the protection of an existing statute to cover a new technology without revising the entire statute to conform to the unique characteristics of the technology. If Congress chooses this method of legislating, it should perform a comprehensive evaluation of the technology to ensure that all of the defined terms and provisions of the existing statute conform to the unique attributes of the new technology.

[228] *See infra* notes 230-54 and accompanying text.

[229] John F. Kennedy, Frankfurt, West Germany (June 25, 1963).

[230] U.S. CONST. amend. IV.

surveillance[231] has dramatically expanded the opportunity for such intrusions.[232] As society further incorporates the use of e-mail via the Internet into our everyday life, it will become the mode of communication families and friends use most to communicate.[233] In the future, courts will call more frequently upon the *Katz* "reasonable expectation of privacy" test and the ECPA to determine the fate of privacy rights implicitly guaranteed by the Fourth Amendment.[234]

To ensure the continued vitality of the Fourth Amendment, this Note argues that the law must advance with technology. Thus, Congress must clarify the distinction between an "electronic communication" in "transit" as opposed to an "electronic communication" held in "electronic storage" to protect a citizen's right of privacy. Otherwise, the precious right implicit in the Fourth Amendment will gradually erode. To address this concern, this Note proposes the following modifications to Title I and Title II. These modifications will equalize the protection that the ECPA gives an "electronic communication" when compared to a "wire" or "oral" communication.[235]

### *A. The Proposed Modifications to Title I*

The ECPA defines the terms used in Title I and Title II in section 2510 of Title I.[236] By rewriting four of these definitions, Congress will clarify the difference between an "electronic communication" in "transit"

---

[231] For information on one device called the Forward Looking Infrared Device (FLIR) which detects heat emanating from certain objects, even if inside the home, see Scott J. Smith, Note, *Thermal Surveillance and the Extraordinary Device Exception: Redefining the Scope of the Katz Analysis*, 30 VAL. U. L. REV. 1071 (1996).

[232] The telephone is the most obvious example because its widespread use made it technologically possible to "intercept" citizens' communications without entering homes or other private places. S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555.

[233] The Internet has experienced phenomenal growth. *See* ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996). In 1981 the Internet linked fewer than 300 computers. *Id.* In 1989 the number of computers stood at fewer than 90,000 and by 1993 that number grew to over 1,000,000 computers. *Id.* In 1997, the number of computers in the United States stands at over 5,640,000 and that does not even include the personal computers people use to access the Internet using a modem. *Id.* In all, 40 million people around the world access the Internet and that number is expected to increase to 200 million Internet users by the year 1999. *Id.*

[234] *See* Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549 (1990). The courts determine the level of privacy and freedom for the whole community when they decide a Fourth Amendment issue. *Id.* at 550. If the courts give law enforcement more investigatory power to use in their quest to apprehend criminals, the effect on privacy rights of the community at large grows in "geometric proportion." *Id.* at 550.

[235] *See infra* notes 236-54 and accompanying text.

[236] *See* 18 U.S.C. § 2510 (1994).

as opposed to an "electronic communication" held in "electronic storage" and will equalize the protection afforded a "wire," "oral," and "electronic" communication so that no formalistic distinctions occur.[237] First, Congress should add *"between the point of origin and the point when the user*[238] *receives any communication,"* as well as *"and such term includes any temporary, intermediate storage incidental to the transmission thereof"* to the definition of "electronic communication" in section 2510 (12),[239] along with a new subsection *(E)*, so that the term reads:

---

[237] This Note argues that by equalizing the protection given to a "wire," "oral," and "electronic" communication, no technology will have an advantage over another. In other words, if all technologies receive the same protection, then Congress will eliminate the formalistic distinctions that occur. For example, adding the human voice to an "electronic communication" might qualify the entire communication as a "wire communication," which means that the communication would receive significantly more protection. *See supra*, notes 139-45 and accompanying text (explaining that a "wire communication" receives more protection than an "electronic communication"). This formalistic distinction occurs because the definition of a "wire communication" specifically includes "any aural transfer made in whole or in part . . . ." 18 U.S.C. § 2510(1) (1994). An "aural transfer" means "a transfer containing the human voice at any point . . . ." 18 U.S.C. § 2510(18) (1994). Moreover, "[t]he conversion of a [human] voice signal to digital form for purposes of transmission does not render the communication non-wire. In other words, the term 'wire communication' includes . . . digitized communications to the extent that they contain the human voice . . . ." S. Rep. No. 99-541, at 12, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566. In contrast, "a communication is an electronic communication . . . if it . . . cannot fairly be characterized as containing the human voice. Communications consisting solely of data . . . are electronic communications." *Id.* at 14, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568. Moreover, the definition of an "electronic communication" specifically reads that it does not include "any wire . . . communication." 18 U.S.C. § 2510(12)(A) (1994).

Formalistic distinctions, such as the one presented above, will not occur if Congress makes three changes to equalize the protection given to an "electronic communication" in relation to a "wire" or "oral" communication. First, Congress must remove section 2516(3) which addresses the authorization for interception of an "electronic communication" and add "electronic communication" to sections 2516(1) and (2), possibly reformulating the list of government officials who may authorize an application for a court "intercept" order as well as the list of crimes that qualify for a court "intercept" order. *See* 18 U.S.C. § 2516 (1994); *see also supra* note 140 and accompanying text. Second, Congress must add an "electronic communication" to sections 2515 and 2518(10)(a) so that the statutory exclusionary rule covers an "electronic communication." *See* 18 U.S.C. §§ 2515, 2518(10)(a) (1994); *see also* Leib, *supra* note 139 (explaining why Congress should add an "electronic communication" to the statutory exclusionary rule and reject the "good faith" exception). Third, and for the purpose of this Note, Congress must clarify the distinction between an "electronic communication" in transit and an "electronic communication" held in "electronic storage." If Congress makes these changes, citizens will have no incentive to use one communication over another, or fear that one provides more protection than another does.

[238] Section 2510(13) defines a "user" as "any person or entity who uses an electronic communication service; and is duly authorized by the provider of such service to engage in such use." 18 U.S.C. § 2510(13) (1994).

[239] For the current definition of "electronic communication," see *supra* note 113.

> "electronic communication" means any transfer *between the point of origin and the point when the user receives any communication* of signs, signal, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, *and such term includes any temporary, intermediate storage incidental to the transmission thereof,* but does not include—
> (A) any wire or oral communication;
> (B) any communication made through a tone-only paging device;
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;
> (E) *any electronic storage of such communication for backup protection (as defined in section 2510 (17)), except as provided for in Title II;*

Second, Congress should remove the language "any electronic storage of such communication" and add *"any temporary, intermediate storage incidental to the transmission thereof, but does not include"* to the definition of a "wire communication" in section 2510(1),[240] along a new subsection *(A)*, so that the term reads:

> "wire communication" means any aural transfer in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or 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 in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes ~~any electronic storage of such communication~~ *any temporary, intermediate storage incidental to the transmission thereof, but does not include—*

[240] For the current definition of a "wire communication," see *supra* note 111.

> *(A) any electronic storage of such communication*[241] *for purposes of backup protection (as defined in section 2510 (17)), except as provided for in Title II;*[242]

The first two proposed definitions have two effects. First, the new definition in 2510(12) clarifies that an "electronic communication" is in transit from the time the sender dispatches the communication until the recipient ("user") receives the communication.[243] Second, the addition of subsection *(E)* to section 2510(12) and subsection *(A)* to section 2510(1) clarifies the difference between both an "electronic communication" and a "wire communication" in transit under Title I, from such communications held in "electronic storage" under Title II, as specified next in the proposed definition of "electronic storage."

Third, Congress should completely redefine the term "electronic storage" in section 2510 (17)[244] to read:

> *"electronic storage" may occur only after an electronic communication service discloses to the user in the initial service agreement that the electronic communication service will store such communication and the user elects to have such communication stored for purposes of backup protection, but such term does not include—*
>
> *(A) any temporary, intermediate storage which is incidental to the transmission of such communication between the point of origin and the point when the user receives such communication;*

The effect of the third proposed definition is to separate a "user's" "reasonable expectation of privacy" into two distinct points in time.[245] The first part consists of the "user's" "reasonable expectation of privacy"

---

[241] Voice mail is an example of a "wire communication" that an "electronic communication service" could store for backup protection once the user receives the communication. Voice mail is a "wire communication" because the communication contains the human voice. *See supra* note 237.

[242] Title II is codified in chapter 121 of the UNITED STATES CODE. *See supra* note 110 and accompanying text.

[243] This effect takes into account the logic that *any* communication is in transit and subject to interception from the time the sender dispatches the communication to the recipient until the recipient receives the communication. The proposed definition incorporates this logic so that an "electronic communication" receives the same protection from interception that a "wire" or "oral" communication receives.

[244] For the current definition of "electronic storage," see *supra* note 198.

[245] For an explanation of the *Katz* "reasonable expectation of privacy" test, see *supra* notes 55-64 and accompanying text.

*before* receipt of the "electronic" or "wire" communication,"[246] while the second part consists of the "user's" "reasonable expectation of privacy" *after* receipt of the "electronic" or "wire" communication.[247] In regard to the effect of the first part on e-mail,[248] proposed subsection 2510(12) and subsection 2510(17) read together impart that a "communication service" is merely a temporary custodian of an "electronic communication" which the "user" has not yet received.[249] But in regard to the second part on

---

[246] A review of the ECPA's legislative history indicates that a communication technology is only included as a protected technology if the general public cannot "intercept" the communication. For example, when Congress passed the ECPA in 1986, the definitions of both a "wire communication" and an "electronic communication" excluded "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), (12) (1986). But in 1994, Congress amended both definitions and removed the exclusion because technological advancements increased a "user's" "reasonable expectation of privacy." 18 U.S.C. § 2510(1), (12) (1994). In addition, the ECPA's legislative history illustrates that Congress addressed the "reasonable expectation of privacy" test in the definition of an "oral communication" in section 2510(2). *See* S. REP. NO. 90-1097, at 57, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2178 (explaining that the definition was intended to reflect the existing law in *Katz*). Under section 2510(2), only when an "oral communication" is "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation . . . ." is such communication protected. 18 U.S.C. § 2510(2) (1994). *See also supra* note 112 for the current definition of an "oral communication." Unlike the definition of an "oral communication," the definition of neither "wire communication" nor an "electronic communication" contain the "reasonable expectation of privacy" language. Thus, a "wire" or an "electronic" communication could possibly violate the ECPA regardless of any "reasonable expectation of privacy" based on their inclusion in the ECPA without the *Katz* language. No case has ever dealt directly with the issue of an e-mail message and a "reasonable expectation of privacy." But the Fourth Amendment would probably require some kind of warrant. *See* H.R. REP. NO. 99-647, at 22 (1986).

[247] At first, this Note was also to argue that an additional subsection be added to Title I, section 2518 (Procedure for interception of wire, oral, or electronic communications). The purpose of the subsection was to give government agents the right to use the backup preservation provisions in section 2704 to preserve unread e-mail or voice mail in a user's mailbox during the interim period when the government agency waited for the approval of a court "intercept" order. However, subsection 2518(7) already allows a government agent, under emergency situations, to "intercept such wire, oral, or electronic communication if an application for an order approving the interception is made . . . within forty-eight hours after such interception has occurred, or begins to occur." 18 U.S.C. § 2518(7) (1994). While this subsection appears adequate, Congress could expand its coverage to maintain the proper balance with the legitimate needs of law enforcement.

[248] In regard to voice mail, the effect of proposed subsection 2510(1) and subsection 2510(17) read together impart that a "communication service" is merely a temporary custodian of a "wire communication" that the "user" has not yet received. *See also infra* notes 249-51.

[249] If the third party is merely the temporary custodian of the information, and not the owner, then the defendant can prevent the government from introducing the evidence based on the Fifth Amendment. OFFICE OF TECHNOLOGY ASSESSMENT, ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 50 (1985).

e-mail,[250] once the "user" receives the communication, one of two things may occur depending on the "user's" election in the initial service agreement. If the "user" elected to have the "electronic communication service" store the communication for backup protection, then the "user's" "reasonable expectation of privacy" diminishes, and Title II applies.[251] But if the "user" did not elect to have the "electronic communication service" store the "electronic communication" for backup protection, the "user" downloads the e-mail to a local computer and the "electronic communication service" automatically deletes any e-mail from the "user's" mailbox upon the "user's" exit from the system.[252] Hence, the Title I prohibition on interception applies.

---

[250] In regard to voice mail, once the "user" receives the "wire communication," one of two choices may occur depending on the "user's" election in the initial service agreement. If the "user" elected to have the "electronic communication service" store the communication for backup protection, then the "user's" "reasonable expectation of privacy" diminishes and Title II applies. But if the "user" did not elect to have the "electronic communication service" store the communication for backup protection, then the "user" listens to the voice mail and deletes the communication, or the "electronic communication service" automatically deletes the received communication upon the "user's" exit. Hence, Title I applies. Otherwise, the initial service agreement can allow the "user" to voluntarily leave a received communication on the system upon the "user's" exit without the "electronic communication service" deleting the received communication, but then Title II would apply.

[251] In analogous situations, a person who relinquishes control to a third party, such as a check to a bank, assumes the risk that the third party will give the information to a law enforcement agency. *See supra*, notes 81-83 and accompanying text (explaining the "assumption of the risk" doctrine). *See also* United States v. Miller, 425 U.S. 435, 437 (1976) (holding that a bank depositor had no protectable Fourth Amendment interests in microfilm records of his financial transactions because by revealing his affairs to the bank, he assumed the risk that such information would be conveyed to the government). But Congress reversed the result in *Miller* in the Right to Financial Privacy Act. 12 U.S.C. § 3401, H.R. REP. NO. 647, 99th Cong. at 23 n.40 (1986). Similarly, the Senate Report recommending passage of the ECPA explicitly states that Title II (chapter 121) was "modeled after" the Right to Financial Privacy Act "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. Thus, Congress intended that Title II protect the privacy expectations of citizens who relinquish control to a third party, and maintain the legitimate needs of law enforcement agencies.

[252] The two main protocols for accessing remote mail are Post Office Protocol ("POP") and Internet Message Access Protocol ("IMAP"). Terry Gray, *Message Access Paradigms and Protocols* (visited March 4, 1998) <ftp://ftp.cac.washington.edu/mail/imap.vs.pop>. The protocols can use any of the three different paradigms for accessing remote mailboxes: "off-line," "on-line," or "disconnected." *Id.* In "off-line" operation, the "user's" mail program fetches the e-mail from the "electronic communication service's" mail server, returns to the computer where the "user's" mail program is operating, and then deletes the e-mail from the mail server. *Id.* In "on-line" operation, the "user's" mail program leaves the e-mail on the "electronic communication service's" mail server and manipulates the

Fourth, Congress should add *"wire or"* to the definition of an "electronic communication system" in section 2510(14)[253] so that the term reads:

> "electronic communication service" means any wire, radio, electromagnetic, photo-optical or photoelectronic facilities for the transmission of *wire or* electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

The effect of the proposed definition in section 2510(14) is relevant to the proposed reforms in section 2703 of Title II.

*B. The Proposed Modifications to Title II*

The ECPA addresses stored "wire" and "electronic" communications in Title II. By modifying two of these sections, Congress will balance the protection afforded an "electronic communication" held in "electronic storage" and a "wire communication" held in "electronic storage" so that the protection is equal. First, Congress should add *"a wire or"* to subsection (a) of section 2703 (Requirements for governmental access) so that subsection 2703(a) reads:

> **(a) Contents of *wire or* electronic communications in electronic storage.**—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of *a wire or* an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or

---

e-mail remotely. *Id.* In "disconnected" operation, the "user's" mail program connects to the "electronic communication service's" mail server, makes a cache copy of selected messages, and then disconnects from the server, later to reconnect and re-synchronize with the mail server. *Id.* Of these different paradigms, POP only uses the "off-line" access paradigm, but IMAP can use all three paradigms. *Id.* Important to this Note, in both "on-line" and "disconnected" access paradigms, e-mail is left on the "electronic communication service's" mail server. Thus, the initial service agreement could provide the "user" two choices. The first choice requires the "electronic communication service" to delete any received e-mail messages left on the system upon the "user's" exit from the system. The second choice allows the "electronic communication service" to provide backup protection for those e-mail messages voluntarily left on the system upon the "user's" exit from the system.

[253] *See* 18 U.S.C. § 2510(14) (1994).

> equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

Second, Congress should add *"wire or"* to subsection (a) (1) of section 2704 (Backup preservation) so that subsection 2704 (a) (1) reads:

> **(a) Backup preservation.**—(1) A governmental entity acting under section 2703(b) (2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the *wire or* electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

Similar to the effect of the proposed changes to Title I, the changes to Title II further clarify the separation between a user's "reasonable expectation of privacy" *before* receipt of the communication and *after* receipt of the communication. *After* the "user" receives a communication, the person must choose whether the "electronic communication service" will store the communication or not. If the "user" elects to have the communication stored, then the government need only comply with the less stringent requirements in Title II. But the government must comply with the more stringent requirements in Title I at anytime *before* receipt of the communication.

### C. *Why Adopt the Proposed Modifications?*

The proposed modifications will improve the Court's Fourth Amendment and ECPA jurisprudence in two distinct ways. First, the proposed modifications will put integrity back into the true historical purpose of the Fourth Amendment because they will ensure citizens that the Fourth Amendment acts as a limitation upon the exercise of

government power. In this sense, the proposed modifications are really a recognition of the reason the Framers of the Constitution drafted the Fourth Amendment—to force government agents to respect a citizen's right of privacy.

The second positive effect is that the proposed modifications will realign the ECPA to more fairly and accurately represent the true historical purpose for the Fourth Amendment. Fourth Amendment rights concerning new communication technologies, such as e-mail, will no longer turn on formalistic distinctions. Instead, the distinctions will be fair and logical so that citizens will be secure in knowing that their communication is free from government interception from the time they speak or type until the time the recipient hears or reads the communication. Consequently, citizens will enjoy the protection granted to them by the Fourth Amendment. The privacy rights implicit in the Fourth Amendment are a vital aspect of our society and citizens should assume that they exist, unless clear and sensible reasons argue otherwise.[254]

## VII. CONCLUSION

The courts have slowly muddied the effectiveness of the Fourth Amendment with numerous subdoctrines that have lost sight of the Amendment's true historical purpose. But Congress must see through the murkiness of Fourth Amendment jurisprudence and focus on the fact that the Fourth Amendment is the one procedural safeguard in the Constitution that protects citizens by preventing the government from abusing its power. This concern motivated Congress to pass the federal wiretap laws. Today, the ECPA is clearly the most important statute dealing with the privacy of e-mail in cyberspace.

Congress wanted the ECPA to represent a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies. But the formalistic distinction between an "electronic communication" in "transit" and an "electronic communication" held in "electronic storage" allows law enforcement agencies to avoid the more stringent requirements for a court "intercept"

---

[254] Professor Weinreb proclaims that Fourth Amendment notions of privacy and security help us develop our personality by permitting us:

> to leave our pajamas on the floor, the bed unmade and dishes in the sink, pictures of secret heroes on the wall, a stack of comic books or love letters on the shelf; it allows us to be sloppy or compulsively neat, to enjoy what we have without exposing [ourselves] to the world.

Weinreb, *supra* note 8, at 53.

order. If law enforcement agencies have the ability to sidestep the court "intercept" order for an "electronic communication," then citizens who communicate by "electronic communication" do not receive the same protection from overzealous law enforcement agents as citizens who communicate by "wire communication" or "oral communication." To prevent this result, Congress should modify the ECPA.

The proposed modifications to the ECPA equalize the protection given to an "electronic communication" when compared to a "wire" or "oral" communication so that law enforcement agents must obtain a court "intercept" order to obtain any communication from the time the sender dispatches the communication until the time the recipient receives the communication. Likewise, law enforcement agents must comply with the less stringent requirements to obtain any communication held in storage. If Congress gives an "electronic communication" the same level of protection as the other forms of communication, the formalistic distinctions will end, and the encouragement of emerging technologies will begin. To encourage citizens' use of e-mail, Congress should restore citizen confidence in e-mail privacy by modifying the ECPA to provide an "electronic communication" the same level of protection that the other forms of communication receive and counteract any further erosion of Fourth Amendment rights.

-Robert S. Steere