Western New England Law Review

Volume 28 *28 (2005-2006)*
Issue 2

Article 7

12-16-2009

THE WIRETAP ACT—RECONCILABLE DIFFERENCES: A FRAMEWORK FOR DETERMINING THE "INTERCEPTION" OF ELECTRONIC COMMUNICATIONS FOLLOWING UNITED STATES V. COUNCILMAN'S REJECTION OF THE STORAGE/TRANSIT DICHOTOMY

Michael D. Roundy

THE WIRETAP ACT—RECONCILABLE DIFFERENCES: A FRAMEWORK FOR DETERMINING THE "INTERCEPTION" OF ELECTRONIC COMMUNICATIONS FOLLOWING *United States v. Councilman*'s Rejection of the Storage/Transit Dichotomy

INTRODUCTION

Electronic communications such as e-mail[1] have ushered in a communications revolution.[2] The Electronic Communications Privacy Act of 1986 ("ECPA")[3] attempted to extend the protections of the existing Wiretap Act[4] to the modern, digital forms of communication.[5] Yet, it has not always been clear when the ECPA's wiretap provisions apply and when they do not.

Imagine that two people are interested in covertly intercepting all of your e-mail communications. The first one, Bob, goes to great expense and difficulty to develop a method of "overhearing" your incoming and outgoing messages while they are actually traveling

---

1. Throughout this Note, "e-mail" is used as a proxy for all forms of electronic communications. *See* Supplemental Brief for the United States at 12, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383), 2004 WL 3201458 (describing e-mail as the "paradigmatic example of electronic communications" under the Wiretap Act). It is the type of electronic communication at issue in many of the cases examined. Moreover, the technical details of how e-mail is transmitted are similar to those of other forms of digital electronic communications.

2. Indeed, billions of e-mail messages are transmitted by American businesses every day. Max Guirguis, *Electronic Mail Surveillance and the Reasonable Expectation of Privacy*, 8 J. TECH. L. & POL'Y 135, 142 (2003). E-mail has, in fact, become "indispensable" to the business world. *Id.*

3. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2522, 2701-2711, 3121-3127 (2000)).

4. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 197 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (2000)). The term "wiretap" dates to more than a century ago and originally referred to connecting to a telegraph or telephone wire in order to monitor communications traveling along the wire. *See* MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 1473 (11th ed. 2003). In current usage, though, the term is no longer restricted to the interception of communications traveling by wire, nor even to telephone and telegraph communications. WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 151 (1998).

5. In particular, the Wiretap Act requires a court order based on a strong, particularized showing of probable cause to believe that the targeted individual has committed or will commit an offense enumerated by the statute, and that wiretap surveillance is likely to yield evidence of such offense. In addition, the Wiretap Act requires close judicial oversight of the entire process. *See infra* Part I.D.

along a wire between computers. It is an exceedingly difficult process, and it takes very expensive equipment to achieve his goal. The second, Alice, has a cheaper solution. She uses off-the-shelf software to alter the mail-delivery software that routes messages to and from your e-mail mailbox. The software waits until the e-mail is no longer traveling along a wire, but is instead in temporary computer storage on the routing computer. The software retrieves your messages from temporary storage, sends a duplicate to a separate e-mail address where Alice can then read all of your e-mail at her leisure, and sends the original message on to its destination. Her method is cheap, efficient, easy, and nearly impossible to detect (at least by you).

Which spy are you more worried about? Is it Bob, who must expend great effort and enormous sums of money to monitor the *wire* your e-mail travels over? Or is it Alice, whose off-the-shelf software can achieve the same end, quickly and at low cost, by monitoring the computer *storage* that your messages are temporarily held in before delivery? Under current wiretap law, Bob's mode of surveillance is unquestionably prohibited, while Alice's low-budget, relatively simple surveillance scheme may or may not be prohibited, depending on the court's interpretation of the meaning of "intercept."

This was the issue presented in *United States v. Councilman*, a recent case in the First Circuit, which held that even Alice's brand of surveillance is prohibited by federal wiretap law.[6] The issue, however, is far from settled. Decisions in several other circuits have found that *any* retrieval from electronic storage, regardless of how temporary and incidental to transmission the storage is, is by definition *not* an intercept (and therefore not prohibited) under federal wiretap law.[7] This Note reviews the development of the "storage test," the First Circuit's rejection of such a test in *Councilman*, and the shortcomings of both approaches. It then proposes an alternative approach and provides an analytical framework for future courts to use in resolving the question whether a given acquisition constitutes an "intercept" within the meaning of the law.

Part I of this Note examines the evolution of wiretap law in America. Part II analyzes how the courts have determined whether and when a given type of electronic communication is intercepted within the meaning of the statute. Prior to 2005, every circuit to

6. 418 F.3d 67 (1st Cir. 2005); *see infra* Part III.
7. *See infra* Part II.B.

have addressed the issue had either adopted or spoken favorably of the storage/transit dichotomy that was first developed in the Fifth Circuit. Part III examines in detail the First Circuit's 2005 *Councilman* decision, which rejected the storage/transit test used by other circuits. Part IV establishes that the storage/transit test must be rejected, notes that *Councilman* provides no definite alternative, and offers such an alternative approach, along with a proposed framework for courts to use in determining whether and when a given electronic communication has been intercepted within the meaning of the statute.

I. BACKGROUND

A. *Brief History of the Right to Privacy in America*

Privacy has been described in many ways. To some, it is one's "interest in not having his affairs known to others."[8] Another theory focuses on the "claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[9] Perhaps most memorably, the right to privacy has been characterized simply as "the right to be let alone."[10]

The intellectual origins of a right to privacy lie in the notion that there is a boundary between the public and private parts of our lives, recognized since the time of the ancient Greeks.[11] It is the separation of these realms that establishes the distinction between those things that should be shown to others and those things that should remain hidden.[12] Even the most ancient of written systems of law, the Hammurabi Code, recognized that certain rights with an aspect of privacy to them were of great importance, to the point of providing the death penalty for the crime of breaking into another man's home.[13] However rooted in the mists of human philosophy and history the right of individual privacy may be, in the modern

8. RICHARD C. TURKINGTON & ANITA L. ALLEN, PRIVACY LAW: CASES AND MATERIALS 73 (West 1999) (quoting RESTATEMENT (FIRST) OF TORTS § 867 (1939)).

9. *Id.* (quoting ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967)).

10. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890). The phrase was repeated by Justice Brandeis in his famous dissent in *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). The coinage of the phrase has been attributed to Judge Thomas Cooley, in about 1880. TURKINGTON & ALLEN, *supra* note 8, at 23.

11. TURKINGTON & ALLEN, *supra* note 8, at 2-3.

12. *Id.* at 10 (quoting an excerpt from HANNA ARENDT, THE HUMAN CONDITION 38-78 (1958)).

13. *Id.* at 7 n.2 (quoting Article 2 of the Code of Hammurabi, which provided: "If

era, the scope of that right is defined by statutory and judge-made law.

A right to privacy was not explicitly recognized in American law until the late nineteenth century, though such a right in various forms was implicitly protected under constitutional principles and common law tort theory.[14] The "right to be let alone" was first identified by Judge Thomas Cooley in the 1880s.[15] In 1890, Samuel Warren and Louis Brandeis used the phrase again in laying out the natural-law foundation of privacy rights and advocating for the explicit recognition of a legally-protected right to privacy.[16] The first explicit judicial recognition of the right to privacy occurred only fifteen years later.[17] The campaign for explicit recognition then languished for decades.

By 1960, Dean William Prosser had identified four main types of tort-based rights to privacy from the case law.[18] The first of these, later incorporated into the Second Restatement of Torts,[19] involved the "intrusion upon [one's] seclusion or solitude, or into his private affairs."[20] It is this sort of violation of privacy that is the concern of wiretap law.[21]

---

a man makes a breach into a house, one shall kill him in front of the breach, and bury him in it").

14. *Id.* at 22 (discussing the First Amendment's rights to free speech, press, and association; the Third Amendment's protection against the quartering of soldiers in one's home; the Fourth Amendment's protections against unreasonable searches and seizures; the Fifth Amendment's right against self-incrimination; and the common law tort protections from nuisance, trespass, and private eavesdropping).

15. *Id.* at 23.

16. *Id.*; *see also* Warren & Brandeis, *supra* note 10, at 193. The Warren and Brandeis article is regarded as one of the most influential pieces of legal scholarship in the history of American law. TURKINGTON & ALLEN, *supra* note 8, at 38.

17. TURKINGTON & ALLEN, *supra* note 8, at 23 (citing Pavesich v. New Eng. Life Ins. Co., 50 S.E. 68 (Ga. 1905), which recognized a legal right of privacy and held that the publication of a person's picture without his or her consent violated that right).

18. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) (describing the four torts as: 1) intrusions on one's seclusion or solitude, or into one's private affairs; 2) public disclosure of embarrassing facts; 3) publicity placing one in a false light; and 4) appropriation of one's name or likeness). Dean Prosser noted that at the time only four states had case law rejecting the right of privacy. *Id.* at 388.

19. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977). The Restatement notes that even if the defendant makes no use of the information obtained, the intrusion alone subjects him to liability. § 652B cmt. b.

20. Prosser, *supra* note 18, at 389.

21. The Restatement (Second) of Torts also specifically provides a wiretapping example: "A, a private detective seeking evidence for use in a lawsuit . . . taps B's telephone wires and installs a recording device to make a record of B's conversations. A has invaded B's privacy." RESTATEMENT (SECOND) OF TORTS § 652B cmt. b, illus. 2, 3 (1977); *see* Rhodes v. Graham, 238 Ky. 225, 229 (1931) (holding that tapping a tele-

B. *Wiretap Law Before 1968*

The Fourth Amendment protects people against unreasonable searches and seizures.[22] In *Boyd v. United States*, the Supreme Court suggested that Fourth Amendment protections might extend beyond the physical invasion of property in the conduct of searches to cover the broader notion of "the privacies of life."[23] When first directly confronted with this question in *Olmstead v. United States*,[24] however, the Court backed away from such a notion and held that without a physical trespass into a private area, no violation of the Fourth Amendment could occur.[25]

In *Olmstead*, the Court's earliest wiretap case, the issue was whether law enforcement's warrantless wiretapping of the defendants' telephone lines was a violation of the Fourth Amendment.[26] The Supreme Court held that there was no violation because the wiretapping had not involved any physical trespass into the defendants' homes or offices.[27] The Court refused to enlarge the Fourth Amendment's language "beyond the possible practical meaning of houses, persons, papers, and effects, or so to apply the words search and seizure as to forbid hearing or sight."[28] Instead, the Court adhered to a literal interpretation, holding that the search could only be of "material things—the person, the house, his papers or his effects."[29]

But the Court spoke with a divided voice, splitting 5-4, with Justice Brandeis delivering a vigorous dissent in defense of privacy rights, almost forty years after his landmark Harvard Law Review article on the subject.[30] In fact, *Olmstead* is now more often remembered for Justice Brandeis's dissent than for the majority's holding.[31] To Justice Brandeis, the invasion of "informational pri-

---

phone line is an invasion of privacy akin to eavesdropping that can serve as the basis for an action for damages); *see also* Hamberger v. Eastman, 106 N.H. 107, 111-12 (1964) (holding that invasion of privacy is an actionable tort, and that installation of a listening device in a bedroom was such an invasion, even if nothing was overheard).

22. U.S. CONST. amend. IV.

23. Boyd v. United States, 116 U.S. 616, 630 (1886).

24. 277 U.S. 438 (1928).

25. *Id.* at 465-66.

26. *Id.* at 455.

27. *Id.* at 465-66.

28. *Id.* at 465.

29. *Id.* at 464.

30. *Id.* at 471 (Brandeis, J., dissenting); *see also* Warren & Brandeis, *supra* note 10, at 193.

31. *See* Anita S. Krishnakumar, *On the Evolution of the Canonical Dissent*, 52 RUTGERS L. REV. 781 (2000) (examining the evolution of dissenting Supreme Court

vacy" was far more alarming than searches and seizures in the physical realm. "As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping."[32]

Congress was more receptive than the Court to the proposition that the American people should be protected from the insidious invasiveness of wiretaps. In 1934, Congress enacted the Federal Communications Act of 1934 (FCA).[33] Section 605 of this Act provided explicit protection against electronic surveillance of private conversations: "[N]o person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person . . . ."[34] In *Nardone v. United States*,[35] the Supreme Court held that the statute prohibited on statutory grounds what the Court had not prohibited on constitutional grounds in *Olmstead*: the government could not use evidence obtained from illegal wiretaps in federal courts.[36]

Section 605 and *Nardone* provided only limited protection, however. First, the Department of Justice interpreted *Nardone* as prohibiting the interception *and* divulgence of private wire communications, but not interception alone, so long as the contents of the messages were not divulged to anyone outside the federal government.[37] Second, the FBI secured presidential authority to conduct extensive wiretapping for national and domestic security purposes.[38] Third, for fifteen years, the Supreme Court held that the

---

opinions that become more famous than majority opinions). The Supreme Court has cited the *Olmstead* dissent since 1945—more than twenty years before the decision was overruled. *Id.* at 798. In fact, the Court cited the *Olmstead* dissent eleven times before overruling the case in *Katz v. United States*, 389 U.S. 347 (1967), and over 40 times since then. *Id.* at 798 n.91.

32. *Olmstead*, 277 U.S. at 476 (Brandeis, J., dissenting).

33. Communications Act of 1934, ch. 652, tit. VI, § 605, 48 Stat. 1064, 1103-04 (1934) (current version at 47 U.S.C. § 605(a) (2000)). While the original § 605 prohibited both unauthorized interception *and* divulging or publishing the contents of the communication, the current version omits prohibition of interception, leaving that act to be covered by the Wiretap Act, and simply prohibits any person "receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof." 47 U.S.C. § 605(a) (2000).

34. § 605, 48 Stat. at 1104.

35. 302 U.S. 379 (1937).

36. *Id.* at 382.

37. DIFFIE & LANDAU, *supra* note 4, at 157.

38. With war on the horizon, FBI Director J. Edgar Hoover convinced President Roosevelt to authorize the use of wiretaps for intelligence purposes for the sake of

federal law was not applicable to the states, and thus did not bar the use of evidence obtained from illegal wiretaps in state courts.[39] Finally, technology provided another means for avoiding the statutory prohibitions on wiretapping. While § 605 prohibited interception of any wire or radio communication, it did not explicitly prohibit other forms of electronic eavesdropping, such as surveillance using hidden microphones.[40]

The decade of the 1960s marked a dramatic turn-around in the battle for protection from warrantless wiretapping. A series of Supreme Court decisions gradually extended the reach of the Fourth Amendment[41] while Congress prepared to implement a fundamental change in the nature of federal wiretap law.[42]

In 1967, the Supreme Court unequivocally established the right to conversational privacy beyond the rigid bounds of a physical intrusion.[43] In *Berger v. New York*,[44] the defendant's conviction was based on evidence obtained from an electronic eavesdropping device that had been placed pursuant to a state-authorized warrant.[45] The Supreme Court held that the state's authorizing statute failed to require sufficient particularity in the scope and duration of the desired warrant to satisfy the Fourth Amendment's constitutional

---

national security. *Id.* at 157-58. After the war, the authority to wiretap for intelligence purposes was renewed, and even broadened, to include purposes of "domestic security" and "subversive activity." *Id.* at 158-61. The full extent of FBI wiretapping during this period remains unclear, but is known to have extended to the surveillance of civil rights leaders, members of the press, Supreme Court justices, senators, and congressmen. *Id.* at 162-63.

39. Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 28 (2003) (citing Schwartz v. Texas, 344 U.S. 199, 203 (1952)). The Supreme Court eventually reversed itself, but did so only two days before the enactment of the federal Wiretap Act in 1968, which would change the entire landscape of wiretap law. *Id.* at 29 n.142 (citing Lee v. Florida, 392 U.S. 378, 385 (1968)).

40. Nor, under *Olmstead*, were other forms of eavesdropping considered Fourth Amendment violations absent a physical trespass. Thus, non-wiretap forms of electronic surveillance, such as microphone surveillance, were regarded as perfectly legal under § 605 and under the Fourth Amendment. *Id.* at 29 (2003); *see also* Goldman v. United States, 316 U.S. 129, 131-33, 135 (1942) (holding that the use of a microphone to overhear the defendant's side of his telephone conversations did not constitute a violation of the federal wiretap law, nor a Fourth Amendment violation, so long as no physical trespass within the confines of a private area was made).

41. *See* Silverman v. United States, 365 U.S. 505 (1961); Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967).

42. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (2000)).

43. *See Berger*, 388 U.S. 41; *Katz*, 389 U.S. 347.

44. *Berger*, 388 U.S. 41.

45. *Id.* at 44-45.

standards.[46] The Court recognized that the use of electronic eavesdropping devices was permissible, but only "under the most precise and discriminate circumstances," and when "the 'commission of a specific offense' was charged."[47] The Fourth Amendment did not render the home or office completely inviolable,[48] but the New York statute failed to satisfy the Fourth Amendment's particularity standard.[49]

Six months after *Berger*, the Supreme Court explicitly rejected *Olmstead*'s physical intrusion test in *Katz v. United States*.[50] In its place, the Court enunciated the "expectation of privacy" concept.[51] In the Court's view, the physical intrusion test obscured the real issue: "the Fourth Amendment protects people, not places."[52] What a person "seeks to preserve as private" is protected under the Fourth Amendment regardless of the presence or absence of any physical intrusion.[53]

Even so, electronic surveillance *could* be constitutionally authorized,[54] but only in certain, narrowly-drawn circumstances. The basis, purpose, and extent of the surveillance must be sufficiently precise and constrained, so as to justify a "very limited search and seizure" for legitimate law-enforcement purposes.[55] The safeguards necessitated by such a covert intrusion into a citizen's privacy required close judicial supervision.[56] Absent a judicial safeguard, even an unquestionable showing of probable cause could not prevent a warrantless search from being held unlawful and "per se unreasonable under the Fourth Amendment."[57]

Justice Harlan, in a concurring opinion, enunciated the new standard of review for Fourth Amendment cases as whether the

---

46. *Id.* at 55-56, 63.
47. *Id.* at 63 (quoting Osborn v. United States, 385 U.S. 323 (1966)).
48. *Id.*
49. *Id.* at 60.
50. Katz v. United States, 389 U.S. 347, 352-53 (1967) (holding that warrantless eavesdropping on conversations in a public telephone booth violated the Fourth Amendment, even absent a physical intrusion).
51. *Id.* at 353.
52. *Id.* at 351.
53. *Id.* at 351-52.
54. *Id.* at 354 (citing Osborn v. United States, 385 U.S. 323, 329-30 (1966)).
55. *Id.* at 354-56.
56. *Id.* at 348.
57. *Id.* at 356-57. The government argued for the creation of a new exception to the warrant requirement, for cases involving surveillance of a telephone booth. *Id.* at 358. The Court rejected this, explicitly holding "the procedure of antecedent justification" (a warrant) to be a constitutional requirement for the kind of electronic surveillance at issue. *Id.* at 359.

person searched had a "reasonable expectation of privacy."[58] This standard has been routinely invoked since *Katz* as the general test for Fourth Amendment violations.[59]

C. *The Wiretap Act of 1968*

Following the enactment of the FCA in 1934, wiretap surveillance was (ostensibly) prohibited under federal law.[60] Congressional investigations in the 1960s into organized crime, however, revealed the need for the legal use of wiretaps by law enforcement in order to combat that problem.[61] Congress finally legalized wiretapping, to a limited extent, in 1968.[62]

The Omnibus Crime Control and Safe Streets Act of 1968 contained a provision entitled "Title III—Wiretapping and Electronic Surveillance," now commonly referred to as the "Wiretap Act," which legalized certain wiretapping when conducted with strong judicial oversight.[63] The Wiretap Act completely revamped the prior wiretap law (§ 605 of the FCA), at once permitting the use of wiretaps and other forms of electronic surveillance under federal law, while also implementing considerable statutory limitations and protections against the abuse of such surveillance.[64]

Congress indicated in its findings a number of concerns that had led it to enact the Wiretap Act.[65] First, Congress found that the use of wiretaps and other devices to overhear wire and oral communications without legal sanction was widespread.[66] Second, the use of such surveillance was a critical aid to law enforcement in fighting crime, especially, organized crime.[67] Third, it was necessary for Congress to establish a uniform system for authorizing the interception of wire or oral communications to ensure that the privacy of

---

58. *Id.* at 360 (Harlan, J., concurring).

59. TURKINGTON & ALLEN, *supra* note 8, at 97.

60. *See supra* notes 33, 34 and accompanying text. As noted, though, this law had not actually prevented the frequent use of wiretaps, for various reasons.

61. DIFFIE & LANDAU, *supra* note 4, at 169-70. But the idea of legislation that would legalize wiretaps for law enforcement purposes was not universally embraced. *Id.* at 170. Police, judges, and state attorneys general from around the nation opposed the creation of federal wiretap laws, as did the Attorney General of the United States at that time. *Id.* at 170-71.

62. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (2000)).

63. Tit. III, 82 Stat. at 211.

64. § 801(b)-(d), 82 Stat. at 211.

65. § 801, 82 Stat. at 211.

66. § 801(a), 82 Stat. at 211.

67. § 801(c), 82 Stat. at 211.

such communications was effectively protected against unauthorized intrusions.[68] Finally, as an additional measure of protection against abuses that would put the privacy of innocent people at risk, Congress prescribed close judicial oversight of authorized communications surveillance, as well as limitations restricting such surveillance to the investigation of certain major and enumerated crimes.[69]

The first line of defense against the abusive use of electronic surveillance is the wiretap authorization process. A wiretap can only be requested by certain designated state or federal prosecuting attorneys.[70] The request must be made to a judge, and must detail the circumstances, the specific criminal offense being investigated, the location to be bugged or tapped, the person whose communications are to be monitored, the type of communication anticipated, and the time frame for the proposed surveillance.[71] In addition, the applicant must convince the judge that other, normal investigative methods have failed or are likely to fail to garner the evidence sought.[72] If the judge is convinced that there is probable cause to believe the contentions of the surveillance application, he or she can issue an order authorizing the surveillance for a period of not more than thirty days.[73] Renewal of a wiretap order for an additional thirty days can be obtained by going through the entire process again.[74] These heightened requirements have led commentators and some judges to refer to the court orders so issued as "super-warrants."[75]

---

68. § 801(b), 82 Stat. at 211.

69. § 801(d), 82 Stat. at 211-12. It is important to note that the National Security Agency's current, controversial program of warrantless foreign-intelligence wiretapping is beyond the scope of this Note. The terrorism-related wiretaps, if subject to any federal statute, would be subject to the provisions of the Foreign Intelligence Surveillance Act, not the domestic Wiretap Act. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, tit. I, §§ 101-111, 92 Stat. 1783-1796 (1978). There is, of course, considerable controversy at present as to whether the NSA wiretaps are subject to statutory limitations, or if they are instead valid under the executive authority of the President of the United States.

70. 18 U.S.C. § 2516 (2000).

71. 18 U.S.C. §§ 2516, 2518 (2000).

72. 18 U.S.C. § 2518(3).

73. 18 U.S.C. § 2518(5). Warrantless national security electronic surveillance continued until the Supreme Court declared such practices unconstitutional in 1972. DIFFIE & LANDAU, *supra* note 4, at 176 (citing United States v. U.S. Dist. Ct. for the E. Dist. of Mich., 407 U.S. 297 (1972)).

74. 18 U.S.C. § 2518(5).

75. *See infra* note 101.

D. *Electronic Communications Privacy Act of 1986*

In the years following the enactment of the Wiretap Act, communications technology underwent dramatic changes.[76] The Wiretap Act had been designed to regulate the communications technology of 1968. By the 1980s, electronic communications (such as e-mail) had become common, and the Wiretap Act simply did not regulate them effectively, if at all. In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA")[77] to bring electronic surveillance of digital communications within the scope of federal law.[78]

The ECPA was enacted to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[79] Given the pace of computer and telecommunications development, the Wiretap Act was regarded by the ECPA's sponsors as "hopelessly out of date" because of its failure to protect the integrity of data communications, electronic mail, cellular and cordless telephone transmissions, and other forms of electronic communication.[80]

To address these modern concerns, the ECPA altered the existing statute in three ways. Title I of the ECPA amended the existing Wiretap Act (chapter 119 of title 18 of the U.S. Code) to include electronic communications within its scope.[81] Title II of the ECPA (called the Stored Communications Act, or SCA) added protections for wire and electronic communications retained in computer storage facilities, because such information did not enjoy either constitutional or statutory protections at the time.[82] Title III of the ECPA addressed the use of pen registers and trap and trace devices.[83] This Note is concerned primarily with the reach of Title

---

76. TURKINGTON & ALLEN, *supra* note 8, at 230.

77. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2522, 2701-2711, 3121-3127 (2000)).

78. TURKINGTON & ALLEN, *supra* note 8, at 230; S. REP. NO. 99-541, at 1 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

79. S. REP. NO. 99-541, at 1 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

80. *Id.* at 2.

81. *Id.* at 3.

82. *Id.*

83. *Id.* Title III of the ECPA is not relevant to this Note. Pen registers do not record the content of wire or electronic communications, but provide the user with collateral information, such as the number dialed, or the number from which a call originates. *Id.* at 46. *See generally* Robert Ditzion, Note, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1321, 1325-35 (2004) (discussing pen-register technologies and applicable legal standards).

I, the Wiretap Act (as amended), and to a limited extent Title II, the SCA.[84]

Title I amended the Wiretap Act in various ways. The two aspects most relevant to this Note are the changes to the definition of "wire communication" under the Act and the addition of the term "electronic communications" to the Act. First, prior to enactment of the ECPA, the definition of "wire communication" in the Wiretap Act read: "any communication made . . . by the aid of wire, cable, or other like connection."[85] The ECPA modified this to: "any aural transfer made . . . by the aid of wire, cable, or other like connection."[86] This change from "communication" to "aural transfer" reflects Congress's intent that wire communications should be limited to communications "which include the human voice at any point between and including the points of origin and reception."[87]

The ECPA also added to the definition of "wire communication" a critical provision, reading, "and such term includes any electronic storage of such communication."[88] The purpose of this language was to indicate that "wire communications in storage like voice mail, remain wire communications," protected by the Wiretap Act.[89] In essence, a "wire communication" was meant to include any communication that could be perceived as a human voice at some point in the process, while "electronic communications" (discussed immediately below) were meant to include all *other* forms of communication employing electronic transmission technologies.[90]

The second relevant change that the ECPA made to the prior Wiretap Act was to include electronic communications within the scope of its protections.[91] The ECPA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical sys-

---

84. This Note will refer to both the pre-ECPA Wiretap Act and Title I of the ECPA as the Wiretap Act. For clarity, the pre-ECPA version will be specifically identified as such when the two versions contain relevant differences. Title II of the ECPA will be referred to as the Stored Communications Act or the SCA.

85. 18 U.S.C. § 2510(1) (1970).

86. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. I, § 101(a), 100 Stat. 1848, 1848 (1986) (codified as amended at 18 U.S.C. § 2510(1) (2000)).

87. S. REP. NO. 99-541, at 11.

88. § 101(a), 100 Stat. at 1848.

89. S. REP. NO. 99-541, at 12.

90. *Id.*

91. *See* § 101(c), 100 Stat. at 1851.

tem" exclusive of certain categories, and in particular, excluding any wire or oral communication.[92] The ECPA also expanded various provisions of the Wiretap Act that had applied only to wire or oral communications to now apply to electronic communications, as well.[93] The essential purpose of adding electronic communications to the Wiretap Act was to update the protections offered by the law in light of technological changes in communications.[94] In particular, Congress wanted to protect the privacy of electronic communications in a way similar to that in which wire communications had been protected by the Wiretap Act since 1968.[95]

Title II of the ECPA, the SCA, added a new chapter to title 18 of the U.S. Code.[96] The SCA makes it unlawful to gain unauthorized access "to a wire or electronic communication while it is in electronic storage" at a facility providing electronic communications services.[97] The statute provides for both criminal penalties and civil damages under a private cause of action.[98] While the Wiretap Act is the portion of the ECPA that is of primary importance to interpreting the meaning of "intercept," it will be shown that the interplay of the SCA with the Wiretap Act is also significant.

II. THE MEANING OF "INTERCEPT"

The question of when the acquisition of an electronic communication constitutes an "intercept" in violation of the Wiretap Act is one that has posed a considerable challenge for the courts. The Wiretap Act is infamous for its lack of clarity,[99] and any reading of the provisions relevant to the meaning of "intercept" introduces inconsistencies.[100] It is not a trivial point of law: if a given acquisition falls within the bounds of the Wiretap Act, a very restrictive judicial application process must be followed to obtain a court order au-

92. § 101(a)(6)(C), 100 Stat. at 1849 (codified as amended at 18 U.S.C. § 2510(12) (2000)).

93. § 101(c), 100 Stat. at 1851 (codified as amended at 18 U.S.C. §§ 2510(5), 2510(8), 2510(9)(b), 2510(11), and 2511-2519 (2000)).

94. S. REP. NO. 99-541, at 1-2.

95. *Id.* at 5.

96. § 201, 100 Stat. at 1860 (adding chapter 121, codified as amended at 18 U.S.C. §§ 2701-2711 (2000)).

97. 18 U.S.C. § 2701(a).

98. 18 U.S.C. §§ 2701(b), 2707.

99. Konop v. Hawaiian Airlines (*Konop I*), 236 F.3d 1035, 1042 (9th Cir. 2001).

100. Konop v. Hawaiian Airlines (*Konop II*), 302 F.3d 868, 887 (9th Cir. 2002) (Reinhardt, J., dissenting).

thorizing surveillance.[101] If an acquisition is *not* an "intercept" under the Wiretap Act, the less rigorous requirements of a court order or ordinary search warrant under the SCA are all that stand between law enforcement and access to the communications.[102] Thus, how the courts choose to interpret the statutory term "inter-

---

101. *See* 18 U.S.C. §§ 2516, 2518. The provisions of § 2518 set a high threshold for the issuing of a court order authorizing interception of wire, oral, or electronic communications. An application for such an order must articulate the particular criminal offense suspected, the location of the place where the interception is to take place, the particular type of communications to be intercepted, and the identity of the person suspected of the offense and whose communications are therefore to be intercepted. 18 U.S.C. § 2518(1)(b). The application must also state in detail the other investigative methods employed, and why such methods have been unsuccessful or will be unlikely to succeed. 18 U.S.C. § 2518(1)(c). For the judge to issue an ex parte court order, he or she must be convinced that there is probable cause to believe that the specified offense has been, is being, or will be committed, and that communications concerning the offense will be obtained through the interception, if authorized. 18 U.S.C. § 2518(3)(a), (b). The judge must also find that normal investigative procedures have been tried and have failed, or would be unlikely to succeed if tried. 18 U.S.C. § 2518(3)(c). Further, each court order must specify all of the information required in the government's application for the order. 18 U.S.C. § 2518(4). Some have taken to referring to these high-threshold court orders for wiretap surveillance as "super warrants." *See In re* Application of the U.S. for an Order, 396 F. Supp. 2d 294, 304-05 (E.D.N.Y. 2005) (noting a hierarchy of legal processes for obtaining court approval of electronic surveillance, placing wiretaps under 18 U.S.C. §§ 2510-2522 at the top of the hierarchy and designating them as "super-warrant," and noting that a wiretap order "requires additional showings not necessary to obtain a more traditional warrant"); *see also* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U. L. REV. 607, 630-31 (2003) (noting Congress's enactment of a "super-warrant" requirement for telephone and Internet surveillance by government agents).

102. Brief on Rehearing En Banc for Senator Patrick J. Leahy as Amicus Curiae Supporting the United States and Urging Reversal, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383), 2004 WL 2707307. In contrast to the court order required of the Wiretap Act, the SCA has a much lower threshold barrier to authorized government access to stored wire and electronic communications: for communications in electronic storage for 180 days or less, the government must obtain an ordinary search warrant, "issued under the Federal Rules of Criminal Procedure or equivalent State" procedures. 18 U.S.C. § 2703(a) (2000). For communications that have been in storage for more than 180 days, the government, depending on whether notice is given, must obtain either an ordinary search warrant, an ordinary administrative subpoena, or a court order. 18 U.S.C. § 2703(b) The court order under this SCA provision carries a substantially lower burden for the government than the one under the Wiretap Act, though. Under the SCA, a court order may be obtained merely "if the governmental entity offers specific and articulable facts showing that there are *reasonable grounds* to believe that the . . . [stored] information sought [is] relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (emphasis added). Thus, the SCA does not require anywhere near the level of particularity or judicial oversight as the Wiretap Act does to obtain disclosure of the communications in question. Indeed, when the FBI executes wiretaps under a valid wiretap order for the interception of e-mail, it usually has the service provider conduct the acquisitions, using methods very similar to those at issue in *Councilman*. Brief for the Appellant at 38, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383), 2003 WL 24014616. The storage test would per-

cept" can have significant consequences for the level of privacy people can enjoy in their electronic communications.

Several courts have looked back to the pre-ECPA interpretation of "intercept" and have attempted to graft that standard onto electronic communications. How these interpretations have played out and evolved over time is explored below by examining the key decisions on the question of precisely what constitutes an "intercept" under the Wiretap Act.

A. *The "Contemporaneous" Standard:* United States v. Turk

The primary pre-ECPA precedent that courts have turned to is *United States v. Turk*.[103] In *Turk*, the defendant was convicted of perjury, in part on the basis of a recorded telephone conversation (a *wire* communication) to which he was a party, and which contradicted his sworn testimony.[104] The recording had been made surreptitiously by the other party to the conversation (who was not acting on behalf of law enforcement).[105] While the making of the recording itself was deemed an interception under the Wiretap Act's definition,[106] it did not constitute a violation of the Act "because § 2511(2)(d) specifically exempts situations in which one party to the conversation is himself the interceptor."[107] But the issue in *Turk* was whether law enforcement's subsequent and unauthorized *replaying* of the recording constituted a separate "intercept" under the Wiretap Act.

The Fifth Circuit held that no distinct interception occurs when a previously recorded conversation is replayed.[108] The main legisla-

---

mit the FBI to continue this method of acquisition, but without the necessity of a wiretap order. *Id.*

103. 526 F.2d 654 (5th Cir. 1976).

104. *Id.* at 656-57.

105. *Id.* at 657.

106. The definition of "intercept" at that time differed from the current version, but its effect on the factual circumstances in *Turk* would be the same under either version of the definition. At the time, the definition read "the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (1970). This differs from the current version's text, which reads "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) (2000). Under either version, the act of recording a private telephone conversation fits the meaning of "intercept" of a wire communication.

107. *Turk*, 526 F.2d at 657. The exemption reads: "It shall not be unlawful . . . for a person not acting under color of law to intercept a wire . . . communication where such person is a party to the communication . . . ." 18 U.S.C. § 2511(2)(d) (2000).

108. *Turk*, 526 F.2d at 659.

tive intent underlying the Wiretap Act was to protect "[individual] privacy against unjustified intrusions."[109] As such, it was "the act of [unauthorized] surveillance and not the literal 'aural acquisition' . . . [that] was at the center of congressional concern."[110] Thus, the court determined that no separate interception of a recorded communication occurred when the recording was later replayed.[111]

In its analysis of the meaning of "intercept," the court suggested what has become known as the contemporaneity standard: interception requires "the contemporaneous acquisition of the communication through the use of [a] device."[112] Later courts would repeatedly refer to *Turk* as establishing, under the pre-ECPA wiretap law, a standard requiring that interception occur *contemporaneously* with the transmission of a wire communication,[113] and many would apply a modified version of contemporaneity as the test for determining when an electronic communication has been intercepted in violation of the post-ECPA Wiretap Act.[114]

B. *The Storage/Transit Dichotomy:* Steve Jackson Games v. U.S. Secret Service

The seminal post-ECPA decision in which "intercept" was construed in the context of electronic communications is *Steve Jackson Games, Inc. v. U.S. Secret Service*.[115] In *Steve Jackson*, the government seized a computer pursuant to an ordinary search warrant, but did not obtain a wiretap order before reading 162 unread, private e-mail messages stored on the computer's hard drive.[116] The Secret Service read and deleted these e-mail messages.[117] The Fifth Circuit considered whether reading the e-mails constituted an "intercept" in violation of the Wiretap Act,[118] and concluded that it did not.[119] The court found that the e-mails were in "electronic storage" when retrieved by the Secret Service, and that "Congress did

109. *Id.* at 658.
110. *Id.* at 659.
111. *Id.*
112. *Id.* at 658.
113. *See* Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 460 (5th Cir. 1994) (quoting *Turk*, 526 F.2d at 658); Konop v. Hawaiian Airlines, Inc. (*Konop II*), 302 F.3d 868, 876 (9th Cir. 2002).
114. *See infra* Part II.B.
115. 36 F.3d 457 (5th Cir. 1994).
116. *Id.* at 459.
117. *Id.*
118. *Id.* at 460.
119. *Id.* at 458.

not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'"[120] This is the now infamous "storage/transit dichotomy."

The court began its analysis by examining the text of the statute. The Wiretap Act 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.'"[121] To determine whether an "acquisition" of an electronic communication had occurred, the court needed to examine the definition of "electronic communication" and decide whether the e-mails in question had been "electronic communications" within the meaning of the Wiretap Act at the time they were acquired from the hard drive.

In amending the previous version of the Wiretap Act to include protections for electronic communications, Congress made certain changes that the *Steve Jackson* court found key. First, the definition of "wire communication" had been revised from "any aural transfer made . . . by the aid of wire, cable, or other like connection" to explicitly stating that the "*term [wire communication] includes any electronic storage of such communication.*"[122] In contrast, the definition for "electronic communication" that was added by the ECPA defined that term only as "any *transfer* of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . but does not include . . . any wire or oral communication."[123] To the court, the most notable feature of these changes to the Wiretap Act was that, unlike the definition for "wire communication," the definition of "electronic communication" did not contain any provision that explicitly included such communications while in electronic storage.[124]

---

120. *Id.* at 461-62.

121. *Id.* at 460 (quoting 18 U.S.C. § 2510(4) (1986)).

122. *Id.* at 461 (quoting 18 U.S.C. § 2510(1)) (emphasis in original). The inclusion of communications in electronic storage in the definition of "wire communication" was struck from the statute by the USA PATRIOT Act in 2001. Pub. L. No. 107-56, § 209(1), 115 Stat. 272, 283 (2001). For purposes of this Note, it is assumed that the pre-2001 version is the one under discussion, unless specifically otherwise noted. While the definition of "wire communication" may have some bearing by analogy on the meaning and scope of "electronic communication" under the statute, ultimately it is not dispositive on the question of how to identify interception of electronic communications under the Wiretap Act.

123. *Steve Jackson*, 36 F.3d at 461.

124. *Id.*

Both "wire communication" and "electronic communication" are described as "transfers,"[125] but only the former explicitly includes "electronic storage" of such communications. The revision to the definition of "wire communication" meant that in addition to prohibiting any acquisition during transfer, the statute also prohibits acquiring wire communications from electronic storage. But "unlike the definition of 'wire communication,' *the definition of 'electronic communication' does not include electronic storage of such communications.*"[126] Since the e-mails at issue had been "in electronic storage" (on the hard drive) at the time they were acquired for reading by the Secret Service, the court held that by the plain language of the statute no interception in violation of wiretap law had occurred.[127] With this, the *Steve Jackson* court established the basic storage/transit dichotomy that many other courts would follow in determining when the acquisition of an electronic communication constitutes an "intercept" in violation of the Wiretap Act.[128]

III. *UNITED STATES V. COUNCILMAN* (2005)

By early 2005, the majority of circuits to have examined the issue had adopted the Fifth Circuit's storage/transit test when interpreting the term "intercept" under the Wiretap Act.[129] In eleven years, no other circuit had openly challenged the narrowing of *Turk*'s contemporaneity standard to a mechanistic determination of whether the communication was "in storage" at the time it was ac-

125. The definition for "wire communication" reads, "any aural *transfer* made by [wire]," and that for "electronic communication" reads, "any *transfer* of [information]." 18 U.S.C. §§ 2510(1), 2510(12) (2000) (emphasis added).

126. *Steve Jackson*, 36 F.3d at 461 (emphasis in original).

127. *Id.* at 461-62.

128. *See* Hall v. Earthlink Network, Inc., 396 F.3d 500, 504 (2d Cir. 2005) (suggesting in dicta its acceptance of the *Steve Jackson* storage/transit standard, though not required to apply such a standard because the facts of the case required decision based on a service-provider exception); Theofel v. Farey-Jones, 359 F.3d 1066, 1077-78 (9th Cir. 2003) (reaffirming *Konop II* and the storage test practically without comment); United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir. 2003) (adopting the *Steve Jackson* storage/transit standard where a private party gained access to files stored on defendant's hard drive and forwarded them to police); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003) (noting the unanimous adoption of the storage test in every circuit to have construed "intercept," and adopting the test itself); Konop v. Hawaiian Airlines, Inc. (*Konop II*), 302 F.3d 868, 876, 878 (9th Cir. 2002) (citing *Steve Jackson* and framing the issue in terms of *Turk*'s contemporaneous-with-communication standard and holding that "contemporaneous" meant, at least, "not while [the communication] is in electronic storage").

129. *See supra* note 128.

quired.[130] This finally changed in the First Circuit case of *United Sates v. Councilman*.[131]

In *Councilman*, an e-mail service provider duplicated the incoming e-mail of its clients and read the duplicates without authorization.[132] The defendant, Bradford Councilman, was the vice president of an Internet company (Interloc, Inc.) that operated an online rare-book listing service.[133] Part of its service was to provide private e-mail accounts for its customers, who were book dealers.[134] In an effort to gain a commercial advantage,[135] Councilman had the company's e-mail delivery software modified so that all messages sent to its customers from Amazon.com would be copied to a separate mailbox before delivery to the intended recipient.[136] The copies were made without permission, before the intended recipients had a chance to read their messages, and while the incoming e-mail messages were in some form of temporary electronic storage.[137] Councilman and other company employees read thousands of these copied e-mail messages.[138] The First Circuit, sitting en banc, held that such acquisitions of e-mail *could* constitute interceptions in violation of the Wiretap Act, and that the district court's dismissal had therefore been in error.[139]

The court addressed two basic issues with respect to the Wire-

130. However, one of the First Circuit's own prior decisions had expressed some skepticism about this approach. *See In re* Pharmatrak, Inc., 329 F.3d 9, 22 (1st Cir. 2003) (invoking the general contemporaneity standard to find "interception" of electronic communications where unauthorized acquisitions had occurred "simultaneously" with the communications, but disapproving in dicta the "less than apt" storage/transit test in light of technological developments since ECPA had been enacted).

131. 418 F.3d 67 (1st Cir. 2005). The U.S. District Court in Massachusetts had held that retrieval from storage of any kind was, by the language of the statute, not an interception. United States v. Councilman, 245 F.Supp. 2d 319, 321 (D. Mass. 2003). The First Circuit's initial review resulted in a panel decision affirming the district court's holding. United States v. Councilman, 373 F.3d 197, 204 (1st Cir. 2004). Later that year, the panel decision was vacated, and a rehearing en banc was granted. United States v. Councilman, 385 F.3d 793 (2004) (per curiam). The en banc opinion, rejecting the storage/transit test, was delivered in August 2005, and is the primary focus of this Note's analysis. *Councilman*, 418 F.3d at 67.

132. *Councilman*, 418 F.3d at 70.

133. *Id.*

134. *Id.*

135. The hoped-for advantages were the development of a list of books that its clients were interested in, and learning about its competitors. *Id.* at 71.

136. *Id.* at 70.

137. *Id.* at 70-71. The parties stipulated that at all relevant times, the e-mails had been in the company computer's random access memory (RAM) or on its hard disks, or both. *Id.* at 71.

138. *Id.* at 70.

139. *Id.* at 85.

tap Act: the meaning of "electronic communication" and the meaning of "intercept."[140] Its principal analysis focused on the former issue, finding that the latter was subsumed within the former because Councilman's only argument against interception was that the messages were not electronic communications at the time of acquisition.[141]

As to the meaning of "electronic communication," the prosecution argued that the meaning was clear from the text of the definition in the statute, and that the definition covered the e-mail messages at issue.[142] Councilman argued, along the same lines as the view underlying the *Steve Jackson* storage/transit dichotomy, that any communication that is even momentarily in electronic storage is technically not an "electronic communication" under the Wiretap Act.[143] The court held that Councilman's reading of the statute was inconsistent with congressional intent, and therefore incorrect.[144]

The court found that the plain text of the Wiretap Act was unclear as to whether a communication in electronic storage, while in the process of being transmitted, fell within the protective scope of the Act.[145] Taken alone, the court found that the statutory definition of "electronic communication" was probably broad enough to cover incoming e-mail messages while they were being processed by the mail system's software.[146] But whether that definition *could* be read alone or had to be considered in parallel with the statutory definition of "wire communication," which specifically includes messages in storage, was an ambiguous matter subject to conflicting interpretations based on dueling canons of construction.[147]

The defendant relied on the canon that Congress's inclusion of particular language in one section of a statute and omission of similar language in a parallel section should be read as a deliberate inclusion and exclusion, respectively, of the matter contained in that language.[148] As noted, the definition for "wire communication" explicitly includes such communications while in electronic storage, but the definition for "electronic communication" lacks such ex-

140. *Id.* at 72, 79.
141. *Id.* at 80.
142. *Id.* at 72.
143. *Id.*
144. *Id.*
145. *Id.* at 76.
146. *Id.* at 72-73.
147. *See id.* at 75 (noting that the two canons were "in tension").
148. *Id.* at 73.

plicit language regarding electronic storage. The defendant read that fact as a deliberate *exclusion* of communications in storage, even transient storage, from the meaning of "electronic communication," and therefore from the protections of the Wiretap Act.[149]

In tension with that canon was another: when Congress explicitly enumerates exceptions to a general prohibition, additional exceptions should not be implied in the absence of clear legislative intent.[150] Since the Wiretap Act lists four specific exceptions to the general definition of "electronic communication,"[151] the additional exception of *all* such communications in any form of electronic storage should not be implied.[152] Thus, at least *some* communications in electronic storage might still be protected "electronic communications" within the meaning of the Wiretap Act. The court concluded that the text was unclear and that applying the conflicting canons of construction did not resolve the ambiguity.[153]

Turning to the legislative history, the court found that the record indicated that the term "electronic communication" was meant to include instances of transient electronic storage that are incidental to the communication process.[154] As such, the argued distinction between "in transit" and "in storage" communications was rejected.[155] In the court's view, the e-mails at issue, while in temporary electronic storage prior to delivery to the recipient's mailbox, were still "electronic communications" within the statute's meaning.[156]

First, the court noted that the original bill's progress toward a final version clearly indicated that the addition of "electronic communications" to the Wiretap Act was meant to provide broad protections for such communications, and that lesser protections for e-mail had been suggested by the Department of Justice, and rejected by Congress.[157] Further, the court noted that the definition of

149. *Id.*

150. *Id.* at 75.

151. *Id.* at 73 n.9 (quoting the exceptions given at 18 U.S.C. § 2510(12) as "(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device . . . or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds").

152. *Id.* at 75.

153. *Id.* at 76.

154. *Id.* at 79.

155. *Id.*

156. *Id.*

157. *Id.* at 76-77 (citing H. REP. NO. 99-647 (1986) in support of a reading providing broad protections for electronic communications such as e-mail).

"electronic storage" was simply intended to provide protection, via the SCA, for residual copies "left behind after transmission," messages stored in the e-mail user's mailbox, copies retained by service providers for billing purposes or as back-ups for its customers, and the like.[158] The court found no evidence to suggest that Congress meant the statute's phrase "incidental to transmission" to exclude the type of storage necessary for the actual transmission process itself from the protective scope of the Wiretap Act.[159]

Finally, the court found no evidence in the congressional record that the addition of the "any electronic storage of such communication" language to the definition of "wire communication" was intended to have any substantive effect on the scope of protections afforded *electronic* communications.[160] The addition of that language first appeared in the Senate markup version, after the House passed the bill without such language, and no Senate cosponsor ever suggested that such language was meant to remove electronic communications from the protections of the statute while briefly in electronic storage along the transmission route.[161] Thus, the court found that the legislative history indicated that the "storage" language in the definition of "wire communication" was simply meant to explicitly protect voice mail messages in storage, and that no substantive impact on the meaning of "electronic communication" was either intended or inferable.[162] The court concluded that the meaning of "electronic communication" included any transient storage that was "intrinsic to the communications process," and expressly rejected the storage/transit distinction.[163]

Next, the court's analysis turned to the meaning of "intercept" under the Wiretap Act. The court rejected Councilman's argument that any communication acquired from electronic storage was by definition not contemporaneous with transmission, and therefore did not constitute an "interception" in violation of the Wiretap

158. *Id.* at 77 (citing the House Hearings and a report by the Office of Technology Assessment). It is important to note that the definitions in § 2510 serve double duty as definitions for terms used in *both* the Wiretap Act and the SCA. Section 2711 of the SCA, entitled "Definitions for chapter," states that "[a]s used in *this* chapter . . . the terms defined in section 2510 [of the Wiretap Act] have, respectively, the definitions given such terms in that section." 18 U.S.C. § 2711(1) (2000) (emphasis added).

159. *Councilman*, 418 F.3d at 77-78.

160. *Id.* at 78.

161. *Id.*

162. *Id.* at 78-79.

163. *Id.* at 79.

Act.[164] The court regarded this argument as essentially the same as, and "entirely subsumed within," the initial argument over whether the definition of "electronic communication" included communications in temporary storage.[165] Since the court had rejected Councilman's argument on *that* question, the argument over "interception" was rendered moot.[166]

Thus, the *Councilman* court rejected the *Steve Jackson* storage/transit test. Instead, the court found that in some circumstances, when electronic storage of a communication is "transient" and "intrinsic" to the communication process, the communication is regarded as an electronic communication within the protections of the Wiretap Act, and thus necessarily still subject to the possibility of interception in violation of the Act.[167]

IV. ANALYSIS

One fact emerges quite clearly from the various courts' discussions of how best to interpret "intercept": no single interpretation is sufficient by itself. In particular, each interpretation fails to resolve the conflict within the statute.[168] The statute should be interpreted in a manner that is most consistent with the legislative intent, even if some conflicts or inconsistencies remain.[169]

The standard of *contemporaneity* provides the best indicator of when an "interception" within the meaning of the statute occurs, but this standard has largely been misapplied in cases involving electronic communications. Once the proper understanding of "contemporaneous" is established, a fairly straightforward framework emerges for analyzing future cases. In the analysis that follows, this Note establishes that the storage/transit test for interception is flawed and must be rejected, that contemporaneity

---

164. *Id.* at 79-80.

165. *Id.* at 80.

166. *Id.* at 79 (noting that Councilman had not provided any alternative argument for finding that the acquisitions were not "interceptions").

167. *Id.*

168. *See* Dorothy Higdon Murphy, Note, United States v. Councilman *and the Scope of the Wiretap Act: Do Old Laws Cover New Technologies?*, 6 N.C. J. L. & TECH. 437, 441 (2005) (asserting that a close reading of the ECPA allows reasonable people to disagree as to the ECPA's meaning).

169. *See* Konop v. Hawaiian Airlines, Inc. (*Konop II*), 302 F.3d 868, 887 (9th Cir. 2002) (Reinhardt, J., dissenting) ("[T]he [relevant] question [is]: which reading is more coherent and more consistent with Congressional intent?"); Murphy, *supra* note 168, at 441-42 (explaining that Congress introduced the ECPA to reflect the broad purpose of the Wiretap Act).

interpreted broadly is the appropriate standard, and that a framework for future analysis emerges from this broader standard.

A. *The Storage/Transit Test Must Be Rejected*

1. Contrary to Congressional Intent, Interception is Virtually Impossible

The technological nature of e-mail and other forms of electronic communication renders the actual interception of such a communication virtually impossible under the storage/transit test. This fact would cause much of the amended Wiretap Act to be effectively inoperative with respect to electronic communications. A reading that would render a significant portion of the statute inconsequential is, of course, to be avoided.[170] Thus, the storage/transit test must be rejected in favor of an alternative that does not render the statute's prohibition meaningless.

E-mail[171] messages are not transmitted from sender to receiver in the same manner as telephone communications. E-mail messages are first broken down into short segments called packets, which are sent from one computer in the network through a series of other computers, until they reach the destination computer.[172] The packets are then reassembled to recreate the original message.[173] Software on the destination computer then directs the message from temporary storage into the more permanent storage that constitutes the intended recipient's "mailbox."[174] In addition, the message may be temporarily reassembled from the packets at some intermediate point between sender and receiver, stored temporarily, and "re-packetized for [another] leg of [its] journey."[175] While en route, the message may not be immediately deliverable, and could therefore be stored for later delivery.[176] Once delivered, the

---

170. *See Konop II*, 302 F.3d at 888; *see also* Haggar Co. v. Helvering, 308 U.S. 389, 394 (1940) ("A literal reading of [a statute] which would lead to absurd results is to be avoided . . . .").

171. As previously mentioned, "e-mail" is used throughout this Note as a proxy for all forms of electronic communications. *See supra* note 1. Thus, if an interpretation fails to protect e-mail as Congress reasonably intended, then the interpretation should be rejected.

172. *See generally* Kerr, *supra* note 101, at 613-16 (describing the technical details of "packet-switched" communications networks).

173. United States v. Councilman, 418 F.3d 67, 69 (1st Cir. 2005).

174. *Id.* at 70.

175. *Id.* (citing J. Klensin, RFC 2821: Simple Mail Transfer Protocol (Apr. 2001) and Jonathan B. Postel, RFC 821: Simple Mail Transfer Protocol (Aug. 1982)).

176. *Id.*

intended recipient retrieves the message from his or her mailbox and can then read, save, or delete the message.[177]

Unlike a phone call, the entire e-mail message is delivered virtually instantaneously, spending an "infinitesimal amount[ ] of time [actually] 'en route.'"[178] Thus, for someone other than the intended recipient to acquire the contents of such a communication, the usual method is to duplicate one of the copies of the message that are held in temporary electronic storage, either at some point en route, or at the destination computer.[179]

If no interception occurs when an electronic communication is acquired from storage, as the *Steve Jackson* test asserts, then "interception of E-mail within the prohibition of the ECPA [would be] virtually impossible."[180] This virtual impossibility would render the

---

177. *Id.*

178. Konop v. Hawaiian Airlines, Inc. (*Konop II*), 302 F.3d 868, 888 (9th Cir. 2002) (Reinhardt, J., dissenting); Nicole Giallonardo, Note, Steve Jackson Games v. United States Secret Service: *The Government's Unauthorized Seizure of Private E-Mail Warrants More Than the Fifth Circuit's Slap on the Wrist*, 14 J. MARSHALL J. COMPUTER & INFO. L. 179, 198 (1995) (citing Sebastian J. Leonardi, *Roadmap to the Internet*, BARRISTER, Spring 1995, at 18).

179. *Konop II*, 302 F.3d at 888.

180. *Id.* (quoting Jarrod J. White, *E-mail@Work.com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1083 (1997)); *see also* United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003) (noting that under the storage test very few acquisitions of electronic communications would be "interceptions" under the statute, and that in fact such interception would be "virtually impossible"); Kristi Belt, Note, *Did Congress Really Intend to Give Investigative Officers Free Reign With Your Personal Electronic Mail?*—Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994), 41 S. TEX. L. REV. 1457, 1472 (2000) (charging that the *Steve Jackson* analysis "fail[s] to take into consideration" the very nature of an e-mail message); Jarrod J. White, *E-Mail@Work.com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1083 (1997) (asserting that under the *Steve Jackson* approach there is but "a narrow window during which an E-mail interception may occur . . . , [and] unless some type of automatic routing software is used . . . , interception of E-mail within the prohibition of the ECPA is virtually impossible"); Giallonardo, *supra* note 178, at 198 (stating that under the *Steve Jackson* approach the Wiretap Act would "not protect e-mail at all" because of the nature of the technology); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 55, 83 (2004) (noting that under the storage/transit test, law enforcement can easily circumvent the super-warrant requirements of the Wiretap Act by simply waiting "perhaps a nanosecond" until the e-mail has reached its final destination, and that under this interpretation the number of investigations that will have to confront wiretap restrictions is reduced to "almost zero"). Regardless of whether interception would be nearly impossible, it would certainly be very unlikely since any hacker intent on acquiring messages could easily avoid prosecution for violating the Wiretap Act by simply making the acquisitions "from the dozens, or even hundreds, of places an electronic communication resides, usually for 'mere nanoseconds,' [on] the Internet." Stephen V. Treglia, *Transitory E-Storage: First Circuit Creates New Legal Concept in* 'Councilman,' N.Y. L.J., Sept. 20, 2005, at 5, 7.

entire set of changes by the ECPA to the prior Wiretap Act largely ineffective, contrary to Congress's intent in enacting the changes.

When Congress enacted the Wiretap Act in 1968, and again when it amended it in 1986, it made clear that the underlying purpose of the law was to protect the expectation of privacy in private communications.[181] The ECPA's revisions were meant to update the Wiretap Act and expand its protections beyond wire and oral communications, to include privacy protections for electronic communications.[182] In particular, Congress was concerned with ensuring the privacy of communications in accordance with the principles embodied in the Fourth Amendment.[183] The storage test clearly defeats this fundamental purpose by making interception of electronic communications "virtually impossible."[184] Therefore, the

---

181. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 801(b), 82 Stat. 197, 211 (1968); S. REP. NO. 99-541, at 2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555; *see also* Belt, *supra* note 180, at 1472, 1474 (noting that e-mail is transmitted to a recipient with the same expectation of privacy as attends telephone calls and ordinary postal-service mail, and asserting that privacy interests "remain constant regardless of the form of the communication"). Arguably, the same reasoning applies regardless of whether an e-mail is "on the wire" or in temporary storage, when that e-mail has not yet been delivered to the intended recipient: the expectation of privacy should be unaffected by these temporary technological distinctions.

182. S. REP. NO. 99-541, at 3; *see also* Belt, *supra* note 180, at 1470; Giallonardo, *supra* note 178, at 198-203 (discussing Congress's intent of protecting the privacy of electronic communications and ensuring the public's confidence in using such forms of communication). Belt identifies Congress's desire to update the Wiretap Act in light of technological and structural changes in the telecommunications industry. Belt, *supra* note 180, at 1470; *see also* S. REP. NO. 99-541, at 5 (stating that "the law must advance with the technology to ensure the continued vitality of the Fourth Amendment"). Omitting wiretap protections while e-mail messages are momentarily in storage at various points along the transmission path would in fact *ignore* the technological and structural developments that make e-mail possible in the first instance. That would clearly be contrary to Congress's stated intent.

183. S. REP. NO. 99-541, at 5. At least one court has explicitly held that the Fourth Amendment's reasonable expectation of privacy in telephone conversations (articulated in Katz v. United States, 389 U.S. 247 (1967)) extends, by analogy, to protect the privacy of e-mail communications. United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996). The congressional intention to protect privacy is not limited to privacy for its own sake; it has also been asserted that Congress intended to protect a *governmental* interest in such privacy—that of encouraging the exchange of ideas and information. Murphy, *supra* note 168, at 441; *see also* Guirguis, *supra* note 2, at 154 (arguing that now that *Olmstead*'s physical intrusion test "no longer controls Fourth Amendment inquiry, it makes no sense to extend constitutional protection to a locked container . . . in transit, and then withhold protections from [encrypted e-mails traveling the Internet]").

184. *See supra* note 180 and accompanying text; Brief for the Center for Democracy and Technology et al. as Amici Curiae Supporting Appellant's Petition for Rehearing and Rehearing En Banc, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383), 2004 WL 2058257 (characterizing the storage test as causing the Wiretap

storage test must be rejected.[185]

2. The Storage/Transit Test Arises From a Misreading of the Statute

In addition to its failure to advance Congress's general purpose in enacting the ECPA, the storage/transit test is the product of an improper reading of the specific statutory language. Language in two sections of the ECPA makes clear that Congress anticipated that at least some acquisitions from electronic storage could constitute "interception" of electronic communications.[186] Furthermore, the legislative history shows that the addition of language pertaining to storage to the definition of "wire communication" was not intended to have any implicit impact on the definition of "electronic communication."

First, two provisions of the ECPA indicate that Congress considered interception by acquiring electronic communications from electronic storage entirely possible.[187] The first section was added as an amendment to the Wiretap Act's definition of "electronic communication" in 1996. In § 2510(12)(D), Congress added the following to the short list of exclusions, things *not* considered electronic communications despite the broad language of the definition: "electronic funds transfer information *stored* by a financial institution in a communications system used for the electronic storage and transfer of funds."[188] If, as *Steve Jackson* held, electronic communications in storage could *never* be "intercepted" under the Wiretap Act, then why would the definition of "electronic communication" need a specific exclusion for stored financial information? The fact

---

Act to be "unhinged" from the Supreme Court's precedent on the Fourth Amendment requirements for electronic surveillance, because it would permit law enforcement to easily circumvent the Wiretap Act and "reduce [it] to almost a nullity").

185. United States v. Oates, 560 F.2d 45, 76 (2d Cir. 1977) ("[D]espite the existence of literal language that might dictate a contrary result, a court should interpret a statute in such a way as to effectuate clear legislative intent.").

186. 18 U.S.C. §§ 2510(D), 2701 (2000).

187. *See infra* text accompanying notes 188-194; *see also* 18 U.S.C. §§ 2510(D), 2701 (2000). Various other sections of the Stored Communications Act also refer to electronic communications that are in electronic storage, demonstrating that the *Steve Jackson* reading of the definition of "electronic communication" as excluding any such communication in storage is without merit. *See, e.g.*, 18 U.S.C. § 2701(a) (referring to an "electronic communication while it is in electronic storage") and § 2703(a) (2000) (entitled "CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE").

188. Antiterrorism and Effective Death Penalty Act of 1996 § 731(1), 18 U.S.C. § 2510(12)(D) (2000) (emphasis added).

that this amendment explicitly excludes certain "stored" information from the definition shows that Congress clearly felt that the existing definition did include at least some such communications while in storage.

The other section of the statute that makes a similar assumption is § 2701 of the SCA.[189] There, the text states that "whoever . . . obtains, alters, or prevents authorized access to a wire or electronic communication *while* it is *in electronic storage* . . . shall be punished as provided [elsewhere]."[190] Subsection (c) then states that the provision just quoted "does not apply with respect to conduct authorized . . . in section . . . 2518 of this title."[191] Section 2518 is the provision of the Wiretap Act describing the process by which an application for court-authorized "interception of a wire, oral, or electronic communication" may be made.[192] Thus, the SCA provides penalties for unauthorized access of *stored* electronic communications, *unless* that access has been authorized under the *interception* provisions of the Wiretap Act.[193] This can only mean that the interception of an electronic communication while it is in electronic storage is possible—a possibility that required making an explicit exception in the text of the SCA. If *no* communication in storage *could* be intercepted, there would be no need for the exception.[194]

The second indication that the storage test is the product of statutory misreading comes from the legislative history. The ECPA's addition of "includ[ing] any electronic storage of such communication"[195] to the definition of "wire communication" was not

189. *See* 18 U.S.C. § 2701; Giallonardo, *supra* note 178, at 183-84.

190. 18 U.S.C. § 2701(a) (emphasis added).

191. 18 U.S.C. § 2701(c).

192. 18 U.S.C. § 2518 (2000).

193. Giallonardo, *supra* note 178, at 197. Giallonardo believes that this exception "indicates that, if the proper warrant is obtained, the government may legally intercept an electronic communication in electronic storage. Therefore, . . . [at least some] stored electronic communications are subject to interception under the Federal Wiretap Act." *Id.* Giallonardo would go so far as to apply the exception to e-mail that had been delivered but not yet read by the intended recipient. *Id.* at 197-98. Whether the protections of the Wiretap Act should extend that far (and this Note does not address that issue), the exception stated in § 2701 still indicates that at least some electronic communications in storage *can* be intercepted.

194. *See* Murphy, *supra* note 168, at 457 (arguing that language throughout the ECPA, similar to that in § 2701, "would make little to no sense" if communications in storage were not included in the coverage).

195. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. I, § 101(a)(6)(C), 100 Stat. 1848, 1849 (1986) (codified as amended at 18 U.S.C. § 2510(1) (2000)).

meant to draw a distinction with "electronic communication," but rather was simply intended to clarify or emphasize the fact that the meaning of "wire communication" was meant to cover stored versions of such communications, such as voice mail.[196]

Because wire communications can take place entirely absent any electronic storage, Congress wanted to indicate clearly that the wiretap law was also meant to cover the storage of such communications, such as in a voice mail system.[197] In contrast, the technology underlying electronic communications makes it impossible for such transfers to occur *without* the use of electronic storage at various points along the transmission path. Thus, no explicit inclusion of electronic storage was needed in the definition of "electronic communication," since reading the text as excluding such intrinsic and inevitable storage would render the wiretap law's protection of electronic communications virtually meaningless.[198]

3. The Storage/Transit Test is the Product of a Faulty Analytic Process

In addition to its problems satisfying legislative intent and the text of the statute itself, the storage test under *Steve Jackson* was the product of faulty legal reasoning. The court in *Steve Jackson* inappropriately relied on a "plain language" approach to interpreting the statute that does not hold up under close examination.[199] There are two basic problems with this approach.

First, even the "plain" reading of the statute's text requires some degree of additional reasoning, beyond simply taking the words (or their absence) at face value. The plain reading argument relies on a canon of construction (that inclusion of language in one provision and omission of that language in another provision is de-

196. United States v. Councilman, 418 F.3d 67, 78-79 (1st Cir. 2005); S. REP. NO. 99-541, at 12 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3566 (describing the purpose of the revision as "to specify that wire communications in storage like voice mail, remain wire communications, and are protected accordingly").

197. Konop v. Hawaiian Airlines, Inc. (*Konop I*), 236 F.3d 1035, 1045 (9th Cir. 2001).

198. *See id.* Indeed, Senator Patrick J. Leahy, the original sponsor for the Senate version of the ECPA, has stated that the storage test is inconsistent with the legislative history and "would essentially render ECPA's extension of [the Wiretap Act] to electronic communications a dead letter." Brief on Rehearing En Banc for Senator Patrick J. Leahy as Amicus Curiae Supporting the United States and Urging Reversal, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383), 2004 WL 2707307.

199. Belt, *supra* note 180, at 1458-59; *see* Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 461-62 (5th Cir. 1994).

liberate and meaningful)[200] and an inference that the omission of "storage from the definition of 'electronic communication'" was meant to indicate complete exclusion of stored electronic communications, including when that storage is a part of the transmission process.[201] Reliance on the canon to support the implicit inference demonstrates that the plain language, by itself, "is not so plain."[202] Indeed, this reliance is not terribly surprising. As the Supreme Court has noted, "linguistic analysis [alone] seldom is adequate when a statute is designed to incorporate fundamental values."[203]

In addition, the definitions for "wire communication" and "electronic communication" are not sufficiently parallel to warrant application of the canon in the first place.[204] The essential basis for *Steve Jackson*'s storage test was the notion that the language of the two definitions should be compared and contrasted in order to infer what Congress intended the statute to cover.[205] But this approach is flawed, because the two definitions are both structurally and temporally dissimilar.[206] The definition of "wire communication" was written, in most of its essentials, for the 1968 version of the Wiretap Act.[207] The clause "and such term includes any electronic storage of such communication" was tacked on to the existing definition when the ECPA was enacted in 1986, but the definition was not otherwise changed, except in minor or irrelevant ways.[208]

In contrast, the definition for "electronic communication" was drafted from scratch almost twenty years after the original Wiretap

---

200. United States v. Councilman, 418 F.3d 67, 73 (1st Cir. 2005) (citing Russello v. United States, 464 U.S. 16, 23 (1983)).

201. *Id.*

202. *Id.*

203. Sabbath v. United States, 391 U.S. 585, 589-90 (1968) (holding that opening an unlocked door violated a statutory prohibition on "breaking open" the door, despite the lack of the use of force, based on constitutional values underlying the statute). Indeed, the values at issue in the statute in *Sabbath* were the very same Fourth Amendment protections that underlie the Wiretap Act, passed in the same year that *Sabbath* was decided. *Id.*; *see supra* notes 181-83 and accompanying text.

204. *Councilman*, 418 F.3d at 74-75.

205. *See* Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 461 (5th Cir. 1994).

206. *Councilman*, 418 F.3d at 75.

207. *Id.* "The revised definition [of wire communication] hews closely to its original definition in the 1968 Wiretap Act." Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 213 (1968).

208. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. I, § 101(a)(1)(D), 100 Stat. 1848, 1848 (1986) (codified as amended at 18 U.S.C. § 2510(1) (2000)); *see also Councilman*, 418 F.3d at 78 (noting that the clause was added to the definition of "wire communication" during Senate markup).

Act, is defined in broad terms, and (unlike "wire communication") contains a listing of four specific exclusions.[209] The definition of "electronic communication" does not include any specific reference to electronic storage, except in one of the narrow, specific, exclusions.[210] Thus, both in terms of when the definitions were written and in terms of their structure, the definitions of "wire communication" and "electronic communication" are not sufficiently parallel to warrant a plain text comparison.[211] Read by itself, *without* comparison to "wire communication," the plain text of the definition of "electronic communication" is ambiguous as to whether at least some messages in temporary storage could be intercepted within the statute's meaning.[212] Therefore, the plain language of the statute is not determinative.

B. *"Intercept" Should Be Determined Using a Broad Contemporaneity Standard*

Having demonstrated the analytic, structural, and substantive flaws of the *Steve Jackson* storage test, the question remains: how *should* "intercept" of electronic communications be determined? Although the court in *Councilman* made the right call in rejecting the *Steve Jackson* storage test, the First Circuit failed to provide any interpretive guidance of its own. This Note argues that the basic contemporaneous-with-transmission standard, unfettered by the storage straightjacket, is the appropriate standard of analysis.[213] In enacting the ECPA, Congress recognized and attempted to protect the expectation of privacy in electronic communications.[214] The contemporaneous-with-transmission interpretation, properly de-

209. *See Councilman*, 418 F.3d at 75, 77. The court also pointed out that the listing of the four exclusions brought a separate canon of construction into play: "Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions *are not to be implied*, in the absence of evidence of a contrary legislative intent." *Id.* at 75 (quoting TRW v. Andrews, 534 U.S. 19, 28 (2001)) (emphasis added). The fact that this canon existed in tension with the inclusion/exclusion canon meant that "[a]pplying [the] canons of construction does not resolve the question." *Id.* at 76.

210. 18 U.S.C. § 2510(12) (2000); *see Councilman*, 418 F.3d at 73.

211. *Councilman*, 418 F.3d at 75.

212. *Id.* at 76.

213. *See* Giallonardo, *supra* note 178, at 206 (stating that the *Steve Jackson* court should have applied the basic *Turk* view of interception, requiring an acquisition simultaneous with the act of communication).

214. *See* S. REP. NO. 99-541, at 5 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

fined, ensures that those expectations of privacy are effectively protected.

The essential kernel of interception, identified in *Turk*, is that the surveillance activity—the acquisition—occurs *at the time of the communication* and thereby causes the communication's contents to become known to the unauthorized person conducting the surveillance.[215] Fundamentally, this is precisely the kind of activity that the Wiretap Act as amended by the ECPA is intended to proscribe: acquisition of communications at the time the communication takes place, regardless of whether it is an oral, wire, or electronic communication.

"Contemporaneous" is not a term of art.[216] It does not appear in the statute,[217] and its first use by the Fifth Circuit in *Turk* was simply a straight-forward, plain-English description of the privacy interest meant to be protected by the Wiretap Act.[218] The language of that court, which expressed concern over "activity engaged in *at the time of* the . . . communication,"[219] has been echoed by several of the courts analyzing contemporaneity since then. They have described the standard as involving a determination of "real-time interception,"[220] an "acquisition during 'flight,'"[221] a simultaneous acquisition,[222] or a "real-time requirement."[223] The various descriptions—real-time, during flight, simultaneous, or at the time of communication—all carry the same basic connotation, that acquiring the contents of a communication while the act or process of communication is occurring must be regarded as a violation of the Wiretap Act.

Not all messages acquired from electronic storage will satisfy this standard. Messages acquired from long-term, post-delivery storage will usually be acquired "a substantial amount of time after" the transmission process has occurred, and thus will not consti-

---

215. *See* United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976). The exact language of *Turk*, in the context of a tape-recorded conversation, was: "activity engaged in at the time of the oral communication which causes such communication to be overheard by uninvited listeners." *Id.* (emphasis added).

216. *See id.* at 659 (noting that "acquisition" in the statute, which the court equated with "contemporaneous," was "used by the Congress neither as a term of art nor as a term of technology").

217. *Id.* at 658.

218. *See id.*

219. *Id.* (emphasis added).

220. United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003).

221. *Id.*

222. *In re* Pharmatrak, Inc., 329 F.3d 9, 22 (1st Cir. 2003).

223. United States v. Councilman, 418 F.3d 67, 80 (1st Cir. 2005).

tute "contemporaneous" acquisitions that violate the Wiretap Act.[224] On the other hand, at least *some* acquisitions from storage will be able to satisfy this real-time version of contemporaneity. Electronic communications will often be *both* in storage and in transit at the same time.[225] When such communications are "acquired while . . . still en route to the intended recipients,"[226] it is practically a truism that such acquisitions are made "at the time of the communication," in real-time, and even "during flight,"[227]—in other words, contemporaneously.

The narrowing of *Turk*'s broad contemporaneity standard to a mechanistic storage inquiry[228] was unnecessary. The courts employing the storage test have found no violation of the Wiretap Act in factual circumstances that would have failed the broader contemporaneity test as well. The facts of *Steve Jackson* (e-mail on a hard drive, after delivery but before being read by the intended recipient), *Konop II* (unauthorized viewing of a website well after it had been posted), *Steiger* (acquisition of files stored on a hard drive), and *Fraser* (employee's e-mail stored on a company hard drive read by the employer) all involved acquisitions of communications that were not in any way "contemporaneous" with the act of communicating.[229] As the First Circuit noted in *In re Pharmatrak*, the other circuits had invoked the contemporaneity standard to exclude acquisitions made "a *substantial amount of time after* material was put into electronic storage."[230] In reality, the courts did not need the

224. *See In re Pharmatrak*, 329 F.3d at 21 (citing *Steiger*, 318 F.3d at 1048-50; Konop v. Hawaiian Airlines, Inc. (*Konop II*), 302 F.3d 868, 872-73 (9th Cir. 2002); and Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 458 (5th Cir. 1994)).

225. United States v. Councilman, 245 F.Supp.2d 319, 321 (D. Mass. 2003), *aff'd by* United States v. Councilman, 373 F.3d 197, 203 (1st Cir. 2004), *vacated, reh'g granted en banc*, 385 F.3d 793 (1st Cir. 2004) (per curiam), *rev'd*, 418 F.3d 67 (1st Cir. 2005).

226. *Councilman*, 418 F.3d at 80.

227. This description may require viewing "flight" in its broad sense, as being somewhere in the process of going from A (sender) to B (recipient).

228. *See* Giallonardo, *supra* note 178, at 198 (describing the storage test as a "narrow interpretation" of interception under the Wiretap Act). *But cf.* Pikowsky, *supra* note 39, at 53 (comparing the *Steve Jackson* rejection of Wiretap Act protections for electronic communications in storage to the "discredited rationale of *Olmstead*, which denied Fourth Amendment protection against wiretaps conducted without a physical trespass").

229. *See* Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 459 (5th Cir. 1994); Konop v. Hawaiian Airlines, Inc. (*Konop II*), 302 F.3d 868, 872-73 (9th Cir. 2002); United States v. Steiger, 318 F.3d 1039, 1043-44 (11th Cir. 2003); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 110 (3d Cir. 2003).

230. *In re* Pharmatrak, Inc., 329 F.3d 9, 21 (1st Cir. 2003) (citing United States v. Steiger, 318 F.3d 1039, 1048-50 (11th Cir. 2003) (emphasis added); *Konop II*, 302 F.3d at 872-73; and Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 458 (5th Cir.

storage/transit dichotomy to find that no "contemporaneous" acquisition had occurred in those cases.[231] In fact, applying the "real-time" understanding of contemporaneous, as described above, would change the rationale *but not the outcome* of those cases. Thus, rejecting the unnecessary storage test in favor of the more logical real-time conceptualization of the contemporaneity standard would bring the application of the Wiretap Act to electronic communications in line with the intent of Congress without seriously undermining the existing case law.

C. *A Framework for Determining Interception*

With the federal circuits now technically in conflict over the proper interpretation of the "intercept" of electronic communications, a framework for analysis is needed to reconcile the opposing views. This Note proposes the use of the contemporaneous-with-communication standard in its broad sense, as first articulated in *United States v. Turk*, and as discussed immediately above.[232] In addition, to aid in the application of this standard, a triad of factors bearing on the question of contemporaneity is suggested.

The first factor to consider is whether the acquisition of an electronic communication occurred when that communication was in electronic storage. Such an acquisition is usually not contemporaneous with the transmission process.[233] Thus, this factor weighs against contemporaneity, and against finding an "intercept" in violation of the Wiretap Act. This is virtually the same test as is currently used by the courts that observe the *Steve Jackson* storage/transit test. The difference is that when characterized as merely one factor in the determination, it is no longer conclusive. The facts of *Councilman* provide the most obvious example of when an acquisition would be considered contemporaneous, despite an acquisition from electronic storage.

1994)) (emphasis added); *see also* Murphy, *supra* note 168, at 454-55 (noting that the issue in *Councilman*, pre-delivery acquisition, had not been faced by prior courts that had relied on the storage test).

231. Brief for the Appellant at 29-30, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383), 2003 WL 24014616 (noting that none of the cases in the other circuits had involved "acquisition of communications *during* transmission," and that therefore any language suggesting a storage test was merely dicta) (emphasis added).

232. *See supra* Part IV.B.

233. *See* Karen Ertel, *E-Mail Intercept Violates Wiretap Law, First Circuit Holds*, TRIAL, Nov. 1 2005, at 83, 85 (describing the facts of *Councilman* as presenting a unique case).

The second factor is whether the electronic communication was acquired prior to reaching its final destination. Given the virtually instantaneous nature of the electronic communications process, when a communication is acquired prior to delivery to its intended recipient, the acquisition is likely to be contemporaneous with the act of communication. Thus, this second factor weighs in favor of an "intercept" in violation of the Wiretap Act.[234] Of course, this factor is not dispositive, either. It is unlikely, for example, that Congress intended for communications that are stored as "dead letters," when undeliverable to their intended recipient, to remain indefinitely protected by the Wiretap Act.[235]

A third important factor to consider is whether the acquisition occurred virtually simultaneously with the communication process. If so, this factor would weigh heavily in favor of finding an "intercept" in violation of the Wiretap Act. When the surveillance method acquires the contents of a private communication virtually at the same instant in which the act of communication is occurring, it should not matter whether the contents were acquired from storage nor whether they were acquired a second or two after delivery to the intended recipient. The function of the ECPA in protecting the privacy of such communications should dictate that such acquisitions are forbidden.

The most important aspect of this series of factors is that none of them is dispositive. They can be used to simplify the initial evaluation of a given acquisition of an electronic communication, but ultimately the courts must exercise reasonable judgment, taking into account the facts and circumstances of each case, in determining whether the acquisition constitutes a *contemporaneous* acquisition in violation of the Wiretap Act. The factors are an aid to that determination, but the standard to be used in deciding whether an "intercept" under the statute has occurred is the real-time, contemporaneous-with-communication standard.

---

234. *See* Murphy, *supra* note 168, at 455 (describing the acquisition of an electronic communication *before* delivery to the intended recipient's mailbox as a "crucial" distinction).

235. *See* United States v. Councilman, 245 F.Supp.2d 319, 321 (D. Mass. 2003), *aff'd by* United States v. Councilman, 373 F.3d 197, 203 (1st Cir. 2004), *vacated, reh'g granted en banc*, 385 F.3d 793 (1st Cir. 2004) (per curiam), *rev'd*, 418 F.3d 67 (1st Cir. 2005) (noting that if retrieval of messages from storage was not uniformly deemed to fail the "intercept" requirement, courts would be required to sort which forms of storage are covered by the statute and which, such as back-up copies and undeliverable messages, are not).

CONCLUSION

The First Circuit's decision in *United States v. Councilman* is in conflict with the strict rule established by other circuits that any acquisition of an electronic communication from any form of storage cannot, by definition, be a violation of the Wiretap Act. This is a consequence of the shortcomings of the so-called storage/transit dichotomy as a rule for interpreting the scope of "interception" under the statute. Over the past decade, various circuits have adopted the storage test, but have applied it to factual circumstances that would not even have satisfied the contemporaneity standard, absent the storage test.[236] Thus, the storage-based narrowing of traditional contemporaneity was unnecessary, and in retrospect inappropriate. Contrary to the legislative intent underlying the ECPA, the storage test renders violation of the Wiretap Act, with respect to electronic communications, virtually impossible.[237] Therefore, the *Steve Jackson* storage/transit test for interception must be rejected, and a new framework for analysis erected in its place.

The contemporaneous-with-transmission standard remains the most appropriate measure of interception under the Wiretap Act. But the term "contemporaneous" is a broad one, not easily reduced to a reliable and consistent, mechanistic test. Courts should evaluate the contemporaneity of an alleged interception on a case-by-case basis, considering all the facts and circumstances of each case. Whether an electronic communication is retrieved from electronic storage, whether the communication has yet been delivered to its intended recipient, and whether the acquisition occurs simultaneous with the transmission process itself are all factors to be considered. They can give courts initial guidance on the question of interception, but the ultimate determination of whether a given acquisition occurred contemporaneous with transmission must rest with the judgment of the courts.

*Michael D. Roundy**

236. *See supra* note 229 and accompanying text.

237. *See supra* text accompanying notes 178-80.

* Thank you to the editors of the Western New England Law Review and to Professor Leora Harpaz for giving considerable guidance in the evolution of this Note. Thanks also to my family for all their support.