3-1-2005


Dorothy Higdon Murphy

Follow this and additional works at: http://scholarship.law.unc.edu/ncjolt

Part of the Law Commons

Recommended Citation

Available at: http://scholarship.law.unc.edu/ncjolt/vol6/iss2/8

This Comments is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Journal of Law & Technology by an authorized administrator of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.

Dorothy Higdon Murphy

I. Introduction

Considerable litigation continues to surround the Electronic Communications Privacy Act\(^2\) ("ECPA") as courts struggle to develop an understanding of how the ECPA will accommodate advances in computer technology, namely electronic communication.\(^3\) The ECPA, enacted by Congress in 1986, consists of two titles. Title I, commonly referred to as the Wiretap Act, pertains to the interception of wire, oral, and electronic communications.\(^4\) Title II, commonly referred to as the Stored Communications Act ("SCA"), applies to stored wire and electronic communication.\(^5\)

Great emphasis is placed on the language of the Wiretap Act. Courts draw a distinction between "wire communication"\(^6\) and "electronic communication"\(^7\) because the definition of wire communication includes "electronic storage"\(^8\) while the definition

---

1 J.D. Candidate, University of North Carolina School of Law, 2006.
3 This Comment will focus on email, a form of electronic communication. As Henry Ford II stated, "[t]he economic and technological triumphs of the past few years have not solved as many problems as we thought they would, and, in fact, have brought us new problems we did not foresee." Quote from Henry Ford II, in THE NEW WEBSTER'S DICTIONARY OF QUOTATIONS AND FAMOUS PHRASES, at 233 (Donald O. Bolander ed., 1987).
5 Id. §§ 2701–2711.
6 Id. § 2510(1).
7 Id. § 2510(12).
8 Id. § 2510(17) (defining "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication").
of electronic communication does not.\footnote{In 2001, in a provision of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act"), Congress amended the definition of "wire communication" to exclude stored communications. The USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 283 (2001). Despite this amendment, confusion remains regarding the interpretation of the Wiretap Act. See discussion infra Part III.B. All references made in this Comment are to the statute prior to amendment, unless otherwise noted.} This distinction is significant in determining if and when electronic communication may be "intercepted."\footnote{18 U.S.C. § 2510(4) (defining "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").} Courts have interpreted this distinction to mean that electronic communication that is in electronic storage cannot be intercepted under the Wiretap Act.\footnote{See, e.g., Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003) (holding that the unauthorized acquisition of the contents of a secure, private website does not constitute an "intercept" under the Wiretap Act because the electronic communication was in electronic storage); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994) (holding that obtaining unread email messages from an electronic bulletin board does not constitute an "intercept" under the Wiretap Act because the email messages were in electronic storage).} The problem in applying the statute is that "[t]echnology has, to some extent, overtaken language. Traveling the [I]nternet, electronic communications are often—perhaps constantly—both 'in transit' and 'in storage' simultaneously, a linguistic but not a technological paradox."\footnote{United States v. Councilman, 245 F. Supp. 2d 319, 321 (D. Mass. 2003).}

In United States v. Councilman,\footnote{373 F.3d 197 (1st Cir. 2004).} the First Circuit Court of Appeals addressed the complex issue of when the Wiretap Act protects electronic communication. In a split decision, the First Circuit upheld the district court ruling, holding that an Internet service provider ("ISP") does not violate criminal wiretap laws when it copies and reads customers' email messages without their consent.\footnote{Id.} The First Circuit reasoned that the intercept provisions of the Wiretap Act did not apply due to the fact that the messages...
were held in electronic storage. As of October 5, 2004, a majority of the First Circuit judges voted to withdraw and vacate their prior judgment and rehear the case en banc.

This Comment examines the First Circuit's decision in Councilman and argues that the court incorrectly interpreted and applied settled law to the unique facts of the case, thereby impermissibly allowing electronic communications that are characterized simultaneously as "in transit" and "in storage" to be acquired by ISPs without violating either the Wiretap Act or the SCA. This Comment proposes that in rehearing the case, the court should avoid a narrow construction of the Wiretap Act because such an interpretation leads to outcomes that are contrary to public policy. Furthermore, in rehearing the case, the court should construe the ECPA as a whole statute, not as two separate titles.

Parts I and II of this Comment examine the statutory background for the discussion. Part I provides an overview of the precursor to the ECPA, the Omnibus Crime Control and Safe Streets Act of 1968, and briefly outlines the historical events leading up to the enactment of the ECPA of 1986. Part II summarizes the amendments made to the Omnibus Crime Control and Safe Streets Act of 1968 by the ECPA of 1986.

Part III of this Comment discusses the Wiretap Act as it relates to interception of electronic communications. This Part considers the flawed reasoning the First Circuit employed in Councilman to determine that the defendant did not "intercept" electronic communications in violation of the Wiretap Act when software, installed at his request, allowed him to intentionally copy and read his customers' private email in order to gain a

---

15 Id.
16 United States v. Councilman, 385 F.3d 793, withdrawing and vacating 373 F.3d 197 (1st Cir. 2004).
17 It is questionable whether the defendant would qualify for the provider exception under 18 U.S.C. § 2701(c)(1) of the SCA. See infra text accompanying note 123.
competitive advantage. This Part further argues that the First Circuit is correct in rehearing *Councilman* en banc because the panel misinterpreted and incorrectly applied settled case law to the unique facts of this case.

Part IV of this Comment examines the issues that the First Circuit should address when rehearing *Councilman*. First, this Part discusses whether the language of the Wiretap Act is ambiguous. Next, this Part explores those issues the court requested that the parties address: (1) "[w]hether the conduct at issue in this case could have been additionally, or alternatively, prosecuted under the Stored Communications Act" and (2) "[w]hether the rule of lenity precludes prosecution in this case." In particular, this Part examines the SCA as it relates to stored electronic communications.

Part V of this Comment discusses the negative implications of the First Circuit’s narrow reading of the Wiretap Act when read in conjunction with the SCA. This Part proposes that courts should take measures necessary to prevent electronic communications from being acquired by ISPs without consequence, under either the Wiretap Act or the SCA. Namely, courts should examine both titles of the ECPA concurrently and implement a test to determine which title of the ECPA is applicable to the electronic communication at issue.

II. **Prior to the Enactment of the ECPA: The Omnibus Crime Control and Safe Streets Act of 1968**

Congress enacted the Omnibus Crime Control and Safe

---

20 *Councilman*, 385 F.3d 793, *withdrawing and vacating* 373 F.3d 197 (1st Cir. 2004).

21 *Id.* Note that the defendant in *Councilman*, relying on the provider exceptions in 18 U.S.C. § 2701(c)(1), made the argument that his conduct was lawful under the SCA and was therefore outside the scope of the Wiretap Act. The First Circuit did not address this argument because it went beyond the charges in the indictment.

22 *Id.*
Streets Act, the precursor to the ECPA, in 1968. Title III of the Omnibus Crime Control and Safe Streets Act was commonly referred to as the Federal Wiretap Act. The purpose of the Federal Wiretap Act was to “prohibit, on the pain of criminal and civil penalties, all interceptions of oral and wire communications, except those specifically provided for in the Act, most notably those interceptions permitted to law enforcement officers when authorized by court order in connection with the investigation of [certain] serious crimes.” These restrictions were intended to protect the important government interest in privacy of communication, “thereby encouraging the uninhibited exchange of ideas and information among private parties.” The Federal Wiretap Act was limited in that it only addressed the interception of wire and oral communications. Prior to the enactment of the ECPA, courts interpreted “intercept” to mean the acquisition of a communication contemporaneous with transmission.

In 1984, Senator Leahy wrote to the Attorney General inquiring as to whether electronic communications were covered by the Federal Wiretap Act. The Department of Justice (“DOJ”) responded by stating that electronic communications are protected from acquisition “only where a reasonable expectation of privacy exists.” The DOJ further noted that “in this rapidly developing area of communications which range from cellular non-wire communication..."
telephone connections to microwave-fed computer terminals, distinctions [whether there does or does not exist a reasonable expectation of privacy] are not always clear or obvious.\(^{30}\)

On September 19, 1985, Senators Leahy and Mathias, dissatisfied with the DOJ’s response, introduced a bill for the ECPA of 1985.\(^{31}\) Pursuant to Congress’s order, the Office of Technology Assessment conducted a study in which they concluded that the legal protections for email in 1985 were “weak, ambiguous, or non-existent,” and “electronic mail remain[ed] legally as well as technically vulnerable to unauthorized surveillance.”\(^{32}\) Following a hearing conducted by the Subcommittee on Patents, Copyrights and Trademarks, a new bill superseded the ECPA of 1985 in order to reflect concerns raised by the Subcommittee.\(^{33}\) On June 19, 1986, Senators Leahy and Mathias introduced the new bill, stating that the existing law is “hopelessly out of date”\(^{34}\) and has failed to keep up with developments in computer technology. After reviewing the bill, the Subcommittee amended it to clarify certain provisions. In a unanimous vote, the Subcommittee sent a favorable report on the ECPA of 1986, as amended, to the full Senate.\(^{35}\)

III. The Electronic Communications Privacy Act of 1986
Amends the Federal Wiretap Act

In 1986, Congress enacted the ECPA in order to update and expand the privacy protections in the 1968 Federal Wiretap Act.\(^{36}\)

\(^{30}\) Id. (citing Oversight on Communications Privacy: Hearing Before the Subcomm. on Patents, Copyrights and Trademarks of the Senate Comm. on the Judiciary, 98th Cong., 2d Sess. 17 (1985)).

\(^{31}\) Id.

\(^{32}\) Id. (citing OFFICE OF TECH. ASSESSMENT, U.S. CONG. FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (1985)).


\(^{35}\) S. REP. NO. 99-541, at 5.

\(^{36}\) Id. at 1; see also Electronic Privacy Information Center, United States v. Councilman, at http://www.epic.org/privacy/councilman/ (Nov. 17, 2004) (on file with the North Carolina Journal of Law & Technology).
The purpose of the ECPA is to "protect against the unauthorized interception of electronic communications . . . [and to] update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." The Subcommittee recognized that computers were used extensively to store and process information and that the "law must advance with the technology to ensure the continued vitality of the fourth amendment."

Prior to the enactment of the ECPA, the Federal Wiretap Act only protected wire and oral communications. The ECPA made a number of changes. It amended (1) the definition of "wire communications" to include wire communications in "electronic-storage," such as voicemail; (2) the definition of "intercept" to cover "electronic communications;" (3) the variety of acts constituting interception from "aural acquisitions" to "aural or other acquisition;" (4) the definitions to include the terms "electronic communication," "electronic communications system," "electronic communication service," and "electronic storage;" and (5) the statute to provide that inadvertent interceptions were deemed not to be crimes under the ECPA.

The ECPA prohibits the intentional interception of wire, electronic, and oral communications. Moreover, the legislative history of the ECPA suggests that Congress sought to protect private electronic communications such as email.

---

37 S. REP. NO. 99-541, at 1.
38 Id. at 5.
39 Due to the breadth of this legislation, this Comment only addresses those amendments relevant to the focus of this discussion.
40 United States v. Councilman, 373 F.3d 197, 210 (1st Cir. 2004) ("Congress included electronic storage in its definition of wire communications because it wanted voicemails to be protected under the Wiretap Act after those messages were delivered.").
IV. Title I of the ECPA: The Wiretap Act

A. Statutory Language and Interpretation

The Wiretap Act addresses the interception of wire, oral, and electronic communications. Subject to certain exceptions, a criminal or civil cause of action under the Wiretap Act exists against any person who:

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication . . .;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; [or]

(d) intentionally uses, or endeavors to use, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.  

The Wiretap Act defines both “wire communications”:

---

45 Id. § 2511(1).
46 Section 2510(1) of the Wiretap Act states:
“Wire communication” means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a
and "electronic communications." The notable difference between the two definitions is that the definition of "electronic communication" does not mention "electronic storage" of electronic communications. Prior to Councilman, a majority of the federal appellate courts held that electronic communications in electronic storage could not be intercepted under the Wiretap Act and viewed the term "intercept" as limited to "acquisition contemporaneous with transmission."

Section 2510(12) of the Wiretap Act states:

"Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;
(B) any communication made through a tone-only paging device;
(C) any communication from a tracking device (as defined in section 3117 of this title); or
(D) electronic funds transfer information stored by financial institution in a communications system used for the electronic storage and transfer of funds.

Section 2510(17) (defining "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication").

E.g., Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003), as amended, (Jan. 20, 2004) (holding that an intercept must occur contemporaneously with transmission); United States v. Steiger, 318 F.3d 1039, 1047–51 (11th Cir. 2003) (holding that an intercept did not occur because there was no contemporaneous acquisition); United States v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997) (holding that in order for the Wiretap Act to be violated contemporaneous acquisition is necessary); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994) (holding that obtaining unread email messages from an electronic bulletin board does not constitute an "intercept" under the Wiretap Act). But see United States v. Smith, 155 F.3d 1051, 1057 n.11, 1058 (9th Cir. 1998) (noting that "[t]o the extent that Turk
B. USA PATRIOT Act

On October 26, 2001, President George W. Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act"). The USA PATRIOT Act amended the Wiretap Act to exclude "electronic storage" from the definition of "wire communications." Despite this amendment, which will sunset on December 31, 2005 unless renewed by Congress, confusion continues to surround the Wiretap Act as it relates to the interception of electronic communication. Notably, cases that have taken into account the amendment made by the USA PATRIOT Act and a case cited by Councilman continue to cause difficulty in determining when electronic communications come under the protection of the Wiretap Act. All references to the Wiretap Act in Councilman apply the statute prior to its amendment.

C. United States v. Councilman

In Councilman, the defendant, Bradford C. Councilman, was vice president of Interloc Inc. ("Interloc"). Interloc was primarily an online bookstore specializing in rare and out-of-print books, but Interloc also acted as an ISP and provided some of its customers with email addresses. The defendant was in charge of

stands for a definition of ‘intercept’ that necessarily entails contemporaneity, it has, at least in the context of wire communications, been statutorily overruled."). 50 The USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 283 (2001). The USA PATRIOT Act passed 98 to 1 in the Senate and 357 to 66 in the House. Because the Wiretap Act and the SCA share definitions, the USA PATRIOT Act amended the SCA as well.

51 Note that one of the cases discussed in this Comment, Konop II, took into account the amendments made by the USA PATRIOT Act and the difficulty in determining when electronic communications come under the Wiretap Act has not been resolved. It has been suggested that the USA PATRIOT Act may indicate that Congress did not intend for the Wiretap Act to protect emails after they have been delivered; however, in Councilman, the email was still in transmission and had not yet been delivered.

52 373 F.3d 197, 198–99 (1st Cir. 2004). In order to send an email, you need a connection to the Internet and an account with an ISP that forwards your email. The data that is passed between the two computers is decoded using computer
managing the ISP and the book dealer subscription list. In January of 1998, the defendant instructed Interloc technicians to configure and install email processing software that would copy and send all email sent from Amazon.com, a competitor, to customers using an Interloc-provided email address, to his personal email account before it arrived in the intended recipient's mailbox. Interloc used a program called procmail as its mail delivery agent ("MDA"), and the systems administrator designed a mail processing code called procmail.rc to "intercept, copy, and store all incoming messages from Amazon.com" before delivering them to the intended recipient. The software copied all of the email messages from Amazon.com while the MDA was in the process of placing the email messages into the recipient's mailbox. The defendant read thousands of emails in order to learn what types of books customers demanded so Interloc could gain an advantage.

The standard protocol used for sending Internet email is called Simple Mail Transfer Protocol ("SMTP"). Where the email passes from one computer, known as a mail server, to another as it travels over the Internet. The data in the message might be broken into smaller packets before it is sent. See Orin S. Kerr, Internet Surveillance Law After the USA PATRIOT Act: The Big Brother that Isn't, 97 Nw. U. L. Rev. 607, 613-14 (2003). When the data is in smaller packets it can move more quickly. The ISP converts the data from the phone line back to digital pulses, and its server interprets the information. When you send an email message, your computer routes it to an SMTP server. Computers pass the packets to each other and the server looks at the email address, determines where to send it, and then forwards it to the recipient's mail server. See J. Klensin, RFC 2821—Simple Mail Transfer Protocol, at http://www.faqs.org/rfcs/rfc2821.html (April 2001) (on file with the North Carolina Journal of Law & Technology). Once the packets arrive at their destination, they are reassembled to form a complete email. An MDA (the one in the instant case is called procmail) places the message into the recipient's mailbox. The email is stored in the recipient's electronic mailbox until the recipient retrieves it. Id.

For a discussion of the process of transmitting email, see Kerr, supra note 52.

It is interesting to note that the First Circuit uses the word "intercept" to describe the action of the defendant before reaching the question of whether his action constituted an intercept, which, interestingly enough, they answer in the negative. The First Circuit's use of the word "intercept" is at times confusing; the court switches back and forth between using "intercept" colloquially and in accordance with its statutory meaning.
over Amazon. As a result, the indictment charged the defendant with conspiring to violate the Wiretap Act. According to 18 U.S.C. § 2511(1)(a), criminal penalties will be imposed on "any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."

The First Circuit held that electronic communications in electronic storage are not covered by the intercept provisions of the Wiretap Act. After further finding that the the electronic communications at issue were in electronic storage, the court concluded that no intercept occurred, and thus the Wiretap Act was not violated.

D. Statutory Interpretation: Narrowing the Scope of the Wiretap Act

In Connecticut National Bank v. Germain, the United States Supreme Court stated that, "[I]n interpreting a statute a court should always turn first to one, cardinal canon before all others . . . [C]ourts must presume that a legislature says in a statute what it means and means in a statute what it says there." The Court went on to note in Germain that "[w]hen the words of a statute are unambiguous, then, this first canon is also the last: 'judicial inquiry is complete.'"

In Councilman, the First Circuit addressed the issue of whether the defendant's activity "was an 'intercept' of a communication within the meaning of the Wiretap Act." The

---

57 Id.
58 Id. at 200.
60 Councilman, 373 F.3d at 203.
61 Id. at 204.
63 Id. at 253–54.
64 Id. at 254 (quoting Rubin v. United States, 449 U.S. 442, 430 (1981)).
65 Councilman at 200 (noting that 18 U.S.C. § 2510(4) (2000) 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").
First Circuit began its analysis of the issue much like the district court by noting the difference between the definitions of "wire communications" and "electronic communications" in the Wiretap Act. As stated earlier, the notable difference between the two is that the definition of "electronic communication" does not mention "electronic storage" of the electronic communications. A well-known canon of statutory interpretation states that when language appears in one section of a statute and not in another, the omission is presumed to be intentional and purposeful. Accordingly, the First Circuit found the language of the statute to be unambiguous and held that "Congress did not intend for the Wiretap Act's interception provisions to apply to communication in electronic storage." By adopting this broad definition of electronic storage, the First Circuit narrowed the scope of the Wiretap Act. In accordance with the First Circuit's interpretation, one can "intercept" a wire communication in storage, however, one cannot "intercept" an electronic communication in storage.

E. Interception of Email During Transmission Versus Access to Email in Storage

After determining that the Wiretap Act was not applicable to electronic communications in electronic storage, the First Circuit considered whether the electronic communications at issue were "in transit" or "in storage." The software installed at the instruction of the defendant copied the email messages in real time while they were in the process of being delivered. While the

---

66 For the Wiretap Act definition of "wire communication," see supra note 46.
67 For the Wiretap Act definition of "electronic communication," see supra note 47.
68 U.S.C. § 2510(17) (2000) (defining "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication").
69 See generally In re Hart, 328 F.3d 45, 49 (1st Cir. 2003); Estate of Bell v. Comm'r, 928 F.2d 901, 904 (9th Cir. 1991).
software obtained the email messages in the course of their delivery, the email messages also existed in the random access memory ("RAM") of Interloc's computer system. The First Circuit characterized these electronic communications as in electronic storage, so the requisite interception was lacking, and the communications did not come within the scope of the protections under the Wiretap Act.

The First Circuit stated that "[o]n the facts of this case, it is clear that the electronic communications in this case were in a form of electronic storage."71 Although the court agreed with the government that the electronic communications at issue were acquired in a different manner than those in *Steve Jackson Games, Inc. v. United States Secret Service* and *Konop v. Hawaiian Airlines, Inc.*,72 it nonetheless dismissed the distinction and held the presence of the words "any temporary, intermediate storage"73 controlled with regard to determining the nature of the electronic communication as either in transmission or in electronic storage.

**F. Misinterpretation and Misapplication of Prior Case Law**

*Steve Jackson Games, Inc. v. United States Secret Service*74 was the first case to address the issue of intercept as it relates to electronic communications under the Wiretap Act. The sole and narrow issue addressed by the Fifth Circuit was "whether the seizure of a computer on which is stored private e-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes an 'intercept' proscribed by 18 U.S.C. § 2511(1)(a)."75 The appellant in this case, Steve

---

71 *Councilman*, 373 F.3d at 203, (emphasis added).

72 See discussion infra Part III.F.


74 36 F.3d 457 (5th Cir. 1994). The Fifth Circuit did not address the SCA because the district court in *Steve Jackson Games* had previously held that the Secret Service violated the SCA by seizing stored electronic communications without complying with the appropriate statutory provisions. Each of the appellants was awarded $1,000 in damages and the Secret Service did not challenge this ruling.

75 *Id.* at 460.
Jackson Games, Inc. ("SJG"), published books, magazines, and games. In the mid-1980s, SJG began operating an electronic bulletin board system named Illuminati. SJG used Illuminati to post information about its business, to communicate with customers, and to allow its customers to send and receive private emails. These private emails were temporarily stored on Illuminati’s hard disk until the customers contacted Illuminati to read their mail. After the customers read their email, they could choose either to save it on Illuminati’s hard drive or to delete it entirely.

In October of 1988, the Director of Network Security Technology began investigating the duplication and distribution of a computerized text file by SJG that contained information about another company’s emergency call system. The director notified the Secret Service in July of 1989 about the unauthorized distribution. In February of 1990, the Secret Service discovered that the information about the emergency call system was available on a bulletin board operated by one of SJG’s employees, who also had the ability to review and delete any data on Illuminati. In late February 1990, a Secret Service agent applied for a warrant to search the employee’s residence and SJG’s premises. The following day, the Secret Service obtained a warrant to search the appellant’s residence. The Secret Service seized the appellant’s computer during the course of the investigation and read and deleted 162 email messages that had not yet been retrieved by their intended recipients.

The district court held that the Secret Service did not “intercept” the email in violation of Wiretap Act because its acquisition of the contents of the electronic communications was not contemporaneous with the transmission of those

---

76 Id. at 458.
77 Id.
78 Id.
79 Id.
80 Id. at 458-59.
81 Id. at 459.
82 See id.
83 Id.
communications. The Fifth Circuit affirmed the district court and held that Congress’s definition of "electronic communication" was meant to exclude electronic communications in storage from the protections of the Wiretap Act and that "the seizure of sent but unretrieved e-mail did not constitute an intercept for purposes of 18 U.S.C. § 2511(a)."

Similarly, in Konop v. Hawaiian Airlines, Inc. ("Konop II"), the Ninth Circuit relied on the analysis in Steve Jackson Games. Konop II dealt with the narrow issue of whether an employer violated either the Wiretap Act or the SCA when he accessed an employee’s secure website. Hawaiian Airlines employed the appellant, Konop, as a pilot. Konop created and maintained a website where he posted various bulletins containing negative content regarding his employer, its officers, and the union. Konop compiled a list of employees who were eligible to access the website and provided them with a user name and password. Once on the website, an eligible person could enter his or her name, create a password, and then click on a button marked "submit," which would indicate acceptance of the terms of use.

---

85 United States v. Councilman, 373 F.3d 197, 202 (1st Cir. 2004) (citing Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461–62 (5th Cir. 1994)).
86 302 F.3d 868 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003) (interpreting the Wiretap Act as amended by the USA PATRIOT Act). In prior history, Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035 (9th Cir. 2001) ("Konop I"), the Ninth Circuit interpreted Wiretap Act before it was amended by the USA PATRIOT Act. In Konop I the Ninth Circuit declined to follow Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994) and held that "[i]the contents of secure websites are ‘electronic communications’ in intermediate storage that are protected from unauthorized interception under the Wiretap Act." Konop I, 236 F.3d at 1048. The USA PATRIOT Act was enacted shortly after the Ninth Circuit withdrew its Konop I opinion on Aug. 28, 2001. This legislation amended the Wiretap Act; the definition of “wire communication” no longer includes “storage.” See USA PATRIOT Act § 209, 115 Stat. at 283.
87 Konop II, 302 F.3d at 874.
88 Id. at 872.
89 Id. at 872–73.
Only registered users were allowed access to the website. Visitors were required to log on to the website with a user name and password. The terms prohibited non-eligible parties like Hawaiian management, from accessing the website. The terms also prohibited any eligible person from showing the contents of the website to anyone else.

In December of 1995, the vice president of Hawaiian Airlines approached one of these eligible people and asked for permission to view the website. The employee agreed to let the vice president access the website using his name. Since the employee had never accessed the website to register, the vice president used the employee’s name to create an account. That same day, the union chairman contacted Konop and informed him that the vice president of Hawaiian Airlines was upset by the information posted on Konop’s website. Konop took the website off-line that same day but restored it the following day. During this time, the vice president of Hawaiian Airlines continued to access and view Konop’s website.

The Ninth Circuit, relying on *Steve Jackson Games*, held that “for a website such as Konop’s to be intercepted in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage.” The court noted that its conclusion was “consistent with the ordinary meaning of ‘intercept,’ which is ‘to stop, seize, or interrupt in progress or course before arrival.’” The Ninth Circuit noted in *Konop II* that [t]here are no Supreme Court cases interpreting the provisions of the Wiretap Act and the Stored Communications Act as they relate to electronic communications, and the court of appeals decisions, in our circuit and others, either do not deal with stored electronic communications, or are

\[90\] *Id.*

\[91\] *Id.* at 873.

\[92\] *Id.*

\[93\] *Id.* at 878.

\[94\] *Id.* (quoting WEBSTER’S NINTH NEW COLLEGIATE DICTIONARY 630 (1985)). The Ninth Circuit explained that “intercept” means “acquiring” the contents of a communication, while access merely involves being in a position to acquire the contents of a communication. *Id.*
superseded by changes in law and technology, or both.\textsuperscript{95}

In \textit{Councilman}, the First Circuit incorrectly interpreted the facts unique to that case to be in line with settled law.\textsuperscript{96} In making its ruling, the court not only relied on the language of the statute but also on the decisions of other circuits. The First Circuit noted that the Fifth Circuit in \textit{Steve Jackson Games} held that "Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'"\textsuperscript{97} The court also noted that in \textit{Konop II}, the Ninth Circuit took a strict view of the phrase "in storage" and held that a violation of the Wiretap Act does not occur when an electronic communication is accessed during storage, even if the acquisition takes place in a split second of storage along the path of transmission.\textsuperscript{98} The First Circuit took settled law that dealt with extremely narrow and specific issues and applied those holdings to the case at bar. The overall effect of this action was to narrow the scope of the Wiretap Act even further than previous cases. The First Circuit's decision in \textit{Councilman} ultimately left email communications, which are at times in storage and in transit simultaneously,\textsuperscript{99} without any protection from interception under the Wiretap Act.

Both cases that the First Circuit relied heavily upon are distinguishable from the facts in \textit{Councilman}. Neither \textit{Steve Jackson Games} nor \textit{Konop II} directly address the issue presented in \textit{Councilman}. \textit{Konop II} dealt with an entirely different issue: communications accessed on a private website by an employer.\textsuperscript{100}

\textsuperscript{95} \textit{Id.} at 891.

\textsuperscript{96} For a criticism of the decision, see Editorial, \textit{Derail E-mail Snooping}, \textit{WASH. POST}, July 2, 2004, at A14 (stating that "email has become too ubiquitous" for \textit{Councilman} to stand), available at http://www.washingtonpost.com/wp-dyn/articles/A22198-2004Jul1.html.

\textsuperscript{97} United States v. Councilman, 373 F.3d 197, 202 (1st Cir. 2004) (quoting \textit{Steve Jackson Games, Inc. v. United States Secret Serv.}, 36 F.3d 457, 462 (5th Cir. 1994)).

\textsuperscript{98} \textit{Id.} (citing \textit{Konop v. Hawaiian Airlines, Inc.}, 302 F.3d 868 (9th Cir. 2002), \textit{cert. denied}, 537 U.S. 1193 (2003)).


\textsuperscript{100} \textit{Konop II}, 302 F.3d at 872–73.
In *Steve Jackson Games*, the email at issue had already been sent and was in the recipient’s mailbox at the time that it was obtained by the Secret Service; it just had not been read by the recipient.\(^{101}\) In other words, the email made its way from computer A to computer B and was in computer B at the time it was obtained. The court characterized this state as “in storage.” *Councilman*, however, deals with electronic communications that were sent via email but obtained *prior* to reaching the intended recipient’s mailbox. This distinction, which the First Circuit failed to consider, is crucial in determining whether the email at issue was in storage or in transit. This issue should have been the main focus of the First Circuit, but it was not addressed by the Fifth, Ninth, or First Circuit.

The First Circuit failed to adequately address whether email messages being processed for delivery are in electronic storage. While the First Circuit took great care in examining the statute and precedent in order to establish that electronic communications in electronic storage are not covered by the Wiretap Act because the requisite interception is missing, it should have carefully crafted its issue to reflect the distinct set of facts presented by *Councilman*. Because the email messages in *Councilman* did not reach the inbox of their intended recipients, the First Circuit should have found that they were not in storage but rather that they were still in transit. However, as noted before, the First Circuit simply stated that, “[o]n the facts of this case, it is clear that the electronic communications in this case were in a form of electronic storage.”\(^{102}\)

V. **First Circuit to Rehear *Councilman* En Banc**

On October 5, 2004, the First Circuit announced that a majority of its judges voted to rehear *Councilman* en banc.\(^{103}\) One

---

\(^{101}\) *Steve Jackson Games*, Inc. v. United States Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994).

\(^{102}\) United States v. Councilman, 373 F.3d 197, 203 (1st Cir. 2004) (emphasis added).

\(^{103}\) United States v. Councilman, 385 F.3d 793 (1st Cir. 2004), *withdrawing and vacating* 373 F.3d 197 (1st Cir. 2004).
of the primary issues that the court will consider in rehearing the case is whether the language of the Wiretap Act is ambiguous. The court also requested that the parties submit supplemental briefs addressing two questions: (1) “[w]hether the conduct at issue in this case could have been additionally, or alternatively, prosecuted under the Stored Communications Act?”104 and (2) “[w]hether the rule of lenity precludes prosecution in this case?”105

A. Whether the Language of the Wiretap Act is Ambiguous

In rehearing the case, the First Circuit must consider whether the language of the Wiretap Act is ambiguous. “Ambiguity exists when a statute is capable of being understood by reasonably well-informed persons in two or more different senses.”106 After a close reading of the statute, it becomes clear that it is possible for well-informed persons reading the Wiretap Act to reasonably disagree as to its meaning.

A majority of the First Circuit held that the Wiretap Act was unambiguous.107 As previously discussed, the court placed great weight on the fact that the definition of “wire communication” included “electronic storage” while “electronic communication” did not. The court stopped its inquiry here, held that the statute was unambiguous, and concluded that “electronic communications” in “electronic storage” are not protected by the Wiretap Act.108

In rehearing the case, the court should extend its analysis by examining the rest of the language of the statute. When the ECPA is examined as a whole, ambiguity is apparent because

104 Id. Note that the defendant in Councilman, relying on the provider exceptions in 18 U.S.C. § 2701(c)(1), made the argument that his conduct was lawful under the SCA and was therefore outside the scope of the Wiretap Act. The First Circuit did not address this argument because it went beyond the charges in the indictment.
105 Id.
107 United States v. Councilman, 373 F.3d 197 (1st Cir. 2004).
108 Id.
different meanings become evident.\textsuperscript{109} The First Circuit should begin by taking a closer look at the structure of the shared definitions in the statute. Namely, the structure of the definition of "wire communication" is different than the structure of the definition of "electronic communication." The definition of "wire communication" contains no exceptions, while the definition of "electronic communication" excludes certain communications that fail to qualify as electronic communications. The list of communications that fail to qualify as electronic communications does not include stored communications. Next, the First Circuit should take note that the language of the statute suggests that electronic communications are not distinct from communications in electronic storage. Multiple sections of the Wiretap Act and the SCA refer to electronic communications in electronic storage;\textsuperscript{110} if communications in electronic storage are excluded from the definition of electronic communication then this language would make little to no sense.

Thus, upon a closer look at the language of the statute, there are at least two reasonable understandings of the language of the Wiretap Act: (1) the definition of electronic communication does not include electronic storage, or (2) the definition of electronic communication does include electronic storage. Accordingly, the Wiretap Act is, on its face, ambiguous. In rehearing the case, in order to resolve the ambiguity, the court should look to the statute as a whole, the objective and purpose to be obtained, and legislative history and intent.\textsuperscript{111}

\textsuperscript{109} SINGER, supra note 106, § 46.05, at 154 (stating that "[a] statute is passed as a whole and not in parts or sections and is animated by one general purpose and intent. Consequently, each part or section should be construed in connection with every other part or section so as to produce a harmonious whole."); see also Cent. Hanover Bank & Trust Co. v. Comm’r, 159 F.2d 167, 169 (2d Cir. 1947) ("There is no more likely a way to misapprehend the meaning of language—be it in a constitution, a statute, a will or a contract—than to read the words literally, forgetting the object which the document as a whole is meant to secure.").

\textsuperscript{110} 18 U.S.C. §§ 2510(17), 2701(a), 2703(a) (2000); see also Supplemental Brief for the United States at 13–14, United States v. Councilman, 373 F.3d 197 (1st Cir. 2004) (No. 03-1383).

\textsuperscript{111} SINGER, supra note 106, § 45.05, at 30–31; see discussion infra Parts I, II, and III.F; see also Magnolia Petroleum Co. v. Carter Oil Co., 218 F.2d 1 (10th
B. Whether the Conduct Could Have Been Prosecuted Under the SCA

1. Title II of the ECPA: The SCA

Title II of the ECPA, commonly referred to as the SCA, addresses access to stored wire and electronic communications. It serves the dual purpose of protecting privacy interests and the Government’s legitimate law enforcement needs. The SCA adopts the same definitions used in the Wiretap Act. Under the SCA, whoever

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

The civil and criminal penalties provided by the SCA are less stringent than those provided for under the Wiretap Act. The SCA excludes from liability conduct that is “authorized by a user of that service with respect to a communication of or intended for that user.”

The SCA applies to two categories of communications:
"those associated with transmission and incident thereto" and those "of a backup variety." The SCA, however, does not apply to messages that are still in transmission. Electronic messages that are in transmission are covered by the Wiretap Act. Thus the difference between the Wiretap Act and the SCA is that the Wiretap Act covers the intentional interception of electronic communications in transit, while the SCA covers intentional access without authorization to stored electronic communications.

In *Steve Jackson Games*, the Fifth Circuit did not directly address the SCA because the district court had previously held that the Secret Service violated the SCA by seizing stored electronic communications without complying with the appropriate statutory provisions. In *Konop II*, the Ninth Circuit reversed and remanded the district court’s holding that Hawaiian Airlines was exempt from liability under § 2701(c)(2). The Ninth Circuit noted that if neither of the employees was a “user” of the website at the time he allowed the vice president of Hawaiian Airlines to access the website, then they could not, under § 2701(c)(2), authorize the vice president’s access to the website.

2. *Councilman* and the SCA

In *Councilman*, count one of the indictment charged the defendant with a violation of 18 U.S.C. § 371 for conspiracy to violate 18 U.S.C. § 2511. In addition to moving to dismiss the indictment for failure to state an offense under the Wiretap Act, the defendant also argued that his conduct was lawful under the SCA and therefore outside of the scope of the criminal provisions of the

---

119 *Steve Jackson Games*, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994). Each of the appellants was awarded $1,000 in damages, and the Secret Service did not challenge this ruling. *Id.*
120 *Konop v. Hawaiian Airlines*, Inc., 302 F.3d 868 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003). The Ninth Circuit noted that the district court did not make any findings on whether the employees actually used Konop’s website. Only a user can authorize a third party’s access to the communication. *Id.*
121 *Id.* at 880.
122 United States v. Councilman, 373 F.3d 197, 199 (1st Cir. 2004).
Wiretap Act. The SCA does not contain any of the special protections afforded by the Wiretap Act. Currently, it is easier for private actors such as Councilman to access private communications under the SCA. The First Circuit noted that the defendant's argument went beyond the charges of the indictment and stated that "[g]iven our reading of the Wiretap Act, we need not comment on this argument."

Additionally, the defendant should have been prosecuted under the SCA. In the absence of a clear delineation between the coverage of the Wiretap Act and the SCA, and given the fact that email can be “in transit” and “in storage” simultaneously, one solution might be to require the government to bring a charge of

---

123 In United States v. Councilman, 245 F. Supp. 2d 319, 320 (2003), the district court addressed the SCA. The District Court noted that electronic communications that are “in storage” are covered by the SCA and that persons violating the SCA are subject to criminal penalties. The district court went on to state that the exemption would apply pursuant to § 2701(c)(1), to a person or entity providing wire or electronic communications service. However, the district court did not address whether the conduct was “authorized,” a preliminary requirement for the exception to apply under § 2701(c)(1). Id.

124 The distinction between classifying an electronic communication as coming under the Wiretap Act or the SCA is crucial when it comes to protection. The Wiretap Act contains procedural protections that go beyond the requirements of the Fourth Amendment and that are not applicable to the SCA. Under the Wiretap Act, (1) officers are only permitted to obtain wiretap orders for investigations that involve a federal felony; (2) in addition to probable cause, officers must give specific information regarding the types of communication that would likely be intercepted, and the steps that they will take to avoid obtaining more information than is necessary to their investigation; (3) the wiretap only lasts for the shorter of thirty days or as long as necessary to obtain the information; (4) the government may be required by the court to provide regular updates and to keep the tapes of the wiretap under seal; (5) the court must notify the target that their communication may have been intercepted; and (6) if any of the rules are violated, the evidence obtained through the wiretap is automatically excluded, even if it does not violate the Fourth Amendment. See 18 U.S.C. §§ 2510–2522 (2000).

125 The special protections afforded by the Wiretap Act are not contained in the SCA. Namely, federal law enforcement agents can obtain such communications merely by obtaining a warrant. Furthermore, outside of the Fourth Amendment, a defendant does not have the right to move to suppress communications that were obtained in violation of the SCA. See 18 U.S.C. §§ 2701–2711 (2000).

126 Councilman, 373 F.3d at 204.
conspiracy to violate the Wiretap Act, 18 U.S.C. § 2511, together with conspiracy to violate the SCA, 18 U.S.C. § 2701, and vice versa. The court would then be able to examine both titles of the ECPA concurrently to determine which more aptly fits the nature ("in transit" or "in storage") of the electronic communication at issue. If the First Circuit had examined the Wiretap Act and the SCA concurrently, perhaps it would have noted that its interpretation of the Wiretap Act prohibited the electronic communications from receiving protection under the Wiretap Act or the SCA. In Councilman, an ISP acquired electronic communications without consequence under the Wiretap Act or the SCA. The electronic communication was not protected under the Wiretap Act because it was in transit and in storage simultaneously and the requisite interception was missing; the acquisition of the electronic communication was not protected under the SCA because the defendant was not indicted under the SCA. However, even if the defendant had been indicted under the SCA, the district court in Councilman suggested that the defendant would qualify for the provider exception under SCA § 2701(c)(1). If the district court is correct, ISPs will be allowed to acquire electronic communications that are simultaneously "in transit" and "in storage" without consequence.

C. Whether the Rule of Lenity Precludes Prosecution in This Case

The rule of lenity is "[t]he judicial doctrine holding that a court, in construing an ambiguous criminal statute that sets out
multiple or inconsistent punishments, should resolve the ambiguity in favor of the more lenient punishment.” In *Beecham v. United States*, the United States Supreme Court noted that in deciding whether a statute is so ambiguous as to warrant the application of the rule of lenity, “our task is not the hopeless one of ascertaining what the legislators who passed the law would have decided had they reconvened to consider petitioners’ particular cases. Rather, it is to determine whether the language the legislators actually enacted has a plain, unambiguous meaning.” Thus the rule of leniency applies only if, “after consulting traditional canons of statutory construction[, the Court is] left with an ambiguous statute.” The Court has also recognized that “[t]he fact that [a criminal statute] has been applied in situations not expressly anticipated by Congress does not demonstrate ambiguity. It demonstrates breadth.”

The First Circuit, with the rehearing in mind, asked the parties to address the question of whether the rule of leniency would preclude prosecution in this case. The applicability of the rule of leniency can be examined on two levels in this case: (1) if the elements of the crime are deemed ambiguous, the rule of leniency would preclude prosecution and (2) if the application of

---

129 *Black's Law Dictionary* 1069 (7th ed. 1999); *see also* 73 *American Jurisprudence 2d* Statutes § 197 (2001) (stating that ambiguities in criminal statutes should be resolved in the defendant's favor).

130 511 U.S. 368 (1994).

131 *Id.* at 374.


134 United States v. Councilman, 385 F.3d 793, *withdrawing and vacating* 373 F.3d 197 (1st Cir. 2004).

135 If on the face of the statute the elements of the crime are ambiguous, the rule of leniency would operate in favor of the defendant to preclude prosecution. Consider the following example: (1) a cause of action is brought under the Wiretap Act; (2) the Wiretap Act is ambiguous—there is a question as to whether communications in electronic storage can be intercepted in violation of the Wiretap Act; (3) there is also a question as to the nature of the electronic communication—whether it is in electronic storage or in transit; (4) under the rule of leniency, viewing the action of the defendant in a light most favorable to him, his actions do not constitute an intercept because the communications were classified as in electronic storage and fall out of the protections of the Wiretap
punishment under one of the titles is ambiguous, the rule of lenity would operate to impose the more lenient punishment.\textsuperscript{136}

\begin{footnotesize}
\textsuperscript{136} When the ECPA is viewed as a whole statute, the acquisition of the electronic communication at issue will fall under either the Wiretap Act or the SCA and be subject to the punishments of the applicable provision. If on the face of the statute the application of punishment is ambiguous, the rule of lenity would operate to impose the more lenient punishment. Under the rule of lenity, if the acquisition of the electronic communication falls under the Wiretap Act, it would be subject to the more lenient punishment under the Wiretap Act, and if the acquisition of the electronic communication falls under the SCA, it would be subject to the more lenient punishment under the SCA. The Wiretap Act and the SCA provide for multiple punishments. The criminal and civil penalties provided by the SCA are less stringent than those provided for under the Wiretap Act.

In \textit{Councilman}, when the rule of lenity is applied to both the Wiretap Act and the SCA, the outcome with regard to criminal penalties is the same—a fine. Violation of the Wiretap Act is punishable by a fine or imprisonment not more than five years, or both. However, ISPs do not intercept, and thus do not violate the Wiretap Act, when they are acting in the ordinary course of business. See \textit{Hall v. Earthlink Network, Inc.}, 2005 U.S. App. LEXIS 1230 (2d Cir. Jan. 25, 2005). If the Wiretap Act is viewed as ambiguous and the rule of lenity is applied in this case, assuming that a violation was found, the lesser punishment of a fine would be imposed. It is unlikely that Councilman’s actions would escape liability by qualifying as “in the ordinary course of business.” The SCA provides that “a person or entity providing electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” \textsuperscript{18 U.S.C. § 2702(a)(1) (2000). In regard to criminal penalties under the SCA, a first offense violation is punishable by a fine or imprisonment not more than one year or both. The SCA also provides that, even in the case of a first offense, “if the offense is committed for the purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act,” it is punishable by a fine or imprisonment not more than five years, or both. \textsuperscript{id. § 2701(b)(1)(A). The SCA excludes from liability “conduct authorized by the person or entity providing a wire or electronic communications service.” Id. § 2701(c)(1). The First Circuit stated that Councilman, in obtaining the emails, did so “seeking to gain a commercial advantage.” United States v. Councilman, 373 F.3d 197, 199 (1st Cir. 2004). That said, the punishment of either a fine or not more than five years
The rule of lenity cannot operate to move a person whose actions qualified under one title of the ECPA into another title of the ECPA. A violation of the Wiretap Act involves interception of electronic communication and is not equal to a violation of the SCA, which involves the intentional, unauthorized access of stored communications. Since violation of these provisions is not equal, a person cannot be taken out of one of these provisions and substituted into the other for the benefit of more lenient punishment.

Under the majority and the dissent's interpretation of the Wiretap Act, the rule of lenity would not be applicable in *Councilman*. According to the majority's interpretation of the Wiretap Act, the rule of lenity would not apply because the Wiretap Act is not ambiguous. In his dissenting opinion, Judge Lipez failed to find the Wiretap Act unambiguous on its face; imprisonment would be applicable. If the court viewed the SCA as ambiguous and found a violation of the SCA, under the rule of lenity, a fine would be imposed as punishment. Under the facts of this case, since Councilman's actions were done in order to gain an advantage over the competition, the multiple punishments proscribed by the Wiretap Act and the SCA would be the same.

In regard to civil penalties, the rule of lenity would operate to produce different results under the Wiretap Act and the SCA. The Wiretap Act allows for appropriate relief, which includes, "(1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection (c) and punitive damages in appropriate cases; and (3) a reasonable attorney's fee and other litigation costs reasonably incurred." 18 U.S.C. § 2520(b). Damages are the greater of either the sum of the actual damages incurred by the plaintiff plus any profits made by the defendant as a result of the violation, or statutory damages of whichever is greater—$100 a day for each day of the violation or $10,000. *Id.* § 2520(c)(2). Under the Wiretap Act, the rule of lenity, if applicable, would operate to impose the lesser of the two penalties. The SCA also allows for the private right of action for any person aggrieved by any violation of the SCA. *Id.* § 2707. Appropriate relief includes "(1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection (c); and (3) a reasonable attorney's fee and other litigation costs reasonably incurred." *Id.* In computing damages, no person entitled to recover shall receive less that $1,000 and in the case of willful or intentional violations, punitive damages may be accessed. *Id.* § 2707(c). So, if the rule of lenity applies, the punishment under the SCA would be less stringent than under the Wiretap Act.

137 United States v. Councilman, 373 F.3d 197 (1st Cir. 2004).
however, he resolved the ambiguity by looking to legislative history and intent.\textsuperscript{138} Judge Lipez noted that the statutory canon relied on by the majority, that when Congress includes certain language in one part of a statute and not in another it is generally presumed that Congress did so intentionally, is itself subject to certain exceptions. According to Judge Lipez, this canon is only used as an aid and must yield when a contrary intent on the part of the lawmaker is apparent.\textsuperscript{139} After a close look at the legislative intent behind the Wiretap Act, Judge Lipez concluded that the text of the Wiretap Act is not as plain as the majority may suggest.\textsuperscript{140} After consulting legislative history and intent, Judge Lipez resolved the ambiguity. The rule of lenity applies where “a reasonable doubt persists about the statute’s intended scope even after resort to the statute’s language, structure, legislative history, and motivating policies.”\textsuperscript{141} Thus, under Judge Lipez’s interpretation of the statute, and the majority’s for that matter, the rule of lenity would not apply.

In \textit{United States v. Ahlers},\textsuperscript{142} the First Circuit held that “a statute is not ambiguous simply because litigants (or even an occasional court) question its interpretation. It is only when no reasonably clear meaning can be gleaned from the text of a statute, leaving courts to guess at what Congress intended, that the rule of lenity comes into play.”\textsuperscript{143} Thus, under the court’s previous reasoning, it would be reasonable to conclude that the rule of lenity would not apply in \textit{Councilman}. With the aid of the traditional

\textsuperscript{138} Id. at 211 (Lipez, J., dissenting opinion). Judge Lipez noted that the purpose of the ECPA was to expand the protections afforded electronic communications. He also stated that the reason the definition of wire communications included electronic storage was to account specifically for voicemail. Judge Lipez’s interpretation of the Wiretap Act is consistent with that of the government—an intercept occurs when one acquires an electronic communication contemporaneous with transmission.

\textsuperscript{139} Id. at 210 (Lipez, J., dissenting opinion).

\textsuperscript{140} For an account of the legislative history behind the ECPA, see discussion \textit{supra} Parts I and II.

\textsuperscript{141} 73 AM. JUR. 2D \textit{Statutes} § 197 (2004) (citing Moskal v. United States, 498 U.S. 103 (1990)).

\textsuperscript{142} 305 F.3d 54 (1st Cir. 2002).

\textsuperscript{143} \textit{Ahlers}, 305 F.3d at 62 (citing United States v. Nippon Paper Indus. Co., 109 F.3d 1, 7 (1st Cir. 1997)).
canons of statutory construction, any ambiguities would be remedied and the rule of lenity is no longer necessary. Ultimately, the rule of lenity would not apply in this case because it is highly unlikely that the court would be unable to resolve the ambiguity after employing the traditional canons of statutory construction.

VI. Negative Implications of the Councilman Reading of the Wiretap Act When Read in Conjunction with the SCA

The First Circuit’s decision in Councilman runs contrary to the stated purpose of the ECPA. The stated purpose of the ECPA is to protect the privacy of communications;144 however, the First Circuit’s interpretation of the Wiretap Act affords email very little to no protection.

Senator Leahy, an influential author of the ECPA, commented on the Councilman decision, stating that:

The 2-to-1 decision by the First Circuit Court of Appeals in a case called United States v. Councilman has dealt a serious blow to online privacy . . . . If allowed to stand, this decision threatens to eviscerate Congress’s careful efforts to ensure that privacy is protected in the modern information age.

[The enactment of the] ECPA was a careful, bipartisan and long-planned effort to protect electronic communications in two forms—from real-time monitoring or interception as they were being delivered, and from searches when they were stored in record systems. We recognized these as different functions and set rules for each based on the relevant privacy expectations and threats to privacy implicated by the different forms of surveillance.

The Councilman decision turned this

distinction on its head.\textsuperscript{145}

As Judge Lipez noted in his dissent, under the majority’s approach, “e-mail would only be subject to the Wiretap Act when it is traveling through cables and not when it is being processed by electronic switches and computers during transit and delivery.”\textsuperscript{146} The broad view taken as to what constitutes a stored electronic communication makes it virtually impossible to intercept email messages.\textsuperscript{147} In characterizing the emails at issue as in electronic

\textsuperscript{145} 150 CONG. REC. S7893-96 (daily ed. July 9, 2004) (statement of Sen. Leahy). \textit{But see} Saul Hansell, \textit{You’ve Got Mail (and Court Says Others Can Read It)}, N.Y. TIMES, July 6, 2004, at C1 (noting that some experts argue that Councilman will have little practical effect, “[w]hile the Councilman ruling would limit the applicability of wiretap laws to e-mail, it appears to apply to a very small number of potential cases”); Cynthia A. Casby, \textit{E-mail Spying May Not Violate the Wiretap Act}, Holland & Knight Intellectual Property and Technology, vol. 7 (Sept. 30, 2004) (noting that the House of Representatives introduced two bills to extend the protection of email privacy to messages in electronic storage), available at http://www.hklaw.com/Publications/Newsletters.asp?ID=502&Article=2727.


\textsuperscript{147} Judge Stephen Reinhardt stated,\textit{[A] reading of the Wiretap Act that includes stored electronic communications in the statute’s “intercept” provision is consistent with the nature of the technology at issue, leaves no unexplained statutory gaps, and renders none of the myriad provisions of either the Wiretap Act or the Stored Communications Act superfluous. Under such a reading, the Wiretap Act would prohibit the interception of electronic communications, both stored and en route, and subject violators to serious penalties. [T]his reading, consistent with Congressional intent as revealed in the legislative history of the statute, rejects the idea that stored electronic
storage, the First Circuit fails to take into account the very nature of email. During transit and delivery, email is constantly stored in some temporary manner.\textsuperscript{148}

The email messages in Councilman were obtained while en route to their destination. In order for an email message to be delivered quickly, it is broken down into packets.\textsuperscript{149} When the MDA, procmail, that is responsible for delivering the email messages to their intended recipients, receives the messages, the email messages exist in the RAM within the computer system. The First Circuit pointed to the existence of the emails in RAM during delivery as constituting storage. This interpretation narrowed the coverage of the Wiretap Act to the point that electronic communications that are capable of being characterized as either "in transmission" or "in storage" because they are in both at the same time, ultimately run the risk of being intercepted without consequence, thus falling out of the protection of both the Wiretap Act and the SCA. For instance, in Steve Jackson Games, the Fifth Circuit held that the received, but unread, email messages were in storage and did not receive protection under the Wiretap Act. One might naively assume that these email messages would receive protection under the SCA but that is not always so clear.\textsuperscript{150}

\begin{flushright}
communications are afforded a lesser degree of protection from interception than stored wire communications.
\end{flushright}


\textsuperscript{148} In addition, the Center for Democracy and Technology, the Electronic Frontier Foundation, the Electronic Privacy Information Center, and the American Library Association filed an amicus brief supporting the appellant's petition for a rehearing en banc. See Brief of Amici Curiae The Center for Democracy and Technology, Inc. et. al. at 2, United States v. Councilman, 373 F.3d 197 (1st Cir. 2004) (No. 03-1383). The brief states that Councilman "effectively rewrites the field of Internet surveillance law in ways that no one in Congress ever imagined" and "unhinges the Wiretap Act from the Fourth Amendment decision it codifies, Berger v. New York, 288 U.S. 41 (1967)." Id.\textsuperscript{149} Kerr, supra note 52.

\textsuperscript{150} In Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432 (W.D. Tex. 1993), the district court held that the Secret Service violated the SCA; the Secret Service did not challenge this ruling. The Fifth Circuit did note that its conclusion that the Secret Service did not violate the Wiretap Act was reinforced by the fact that the SCA more appropriately applied to their conduct.
Some courts have held that the definition of storage limits the protection afforded email messages to intermediate storage before delivery,\textsuperscript{151} while other courts have held that the protection afforded email messages in storage also applies to an email's post-transmission storage.\textsuperscript{152}

The First Circuit noted that the "intersection of the Wiretap Act and the Stored Communications Act 'is a complex, often convoluted, area of the law.'"\textsuperscript{153} While the statement is true, this does not mean that courts should permit acquisition of electronic communications without consequence. Courts should not be able to define the nature of an electronic communication so as to avoid application of the protections of the Wiretap Act and the SCA. Because electronic communications are in transit and storage simultaneously,\textsuperscript{154} courts could potentially define the electronic communications as in electronic storage in order to avoid the protections of the Wiretap Act and at the same time, as in the process of being delivered or in transmission to avoid the SCA.

In order to prevent ISPs from acquiring electronic communications without consequence, courts should take measures to protect electronic communications. In hearing cases involving electronic communication, courts should examine the

In cases such as these, the Fifth Circuit noted the importance of construing the ECPA as a whole.

\textsuperscript{151} In re Doubleclick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 511–12 (S.D.N.Y. 2001) (dismissing a class action against largest provider of Internet advertising products and services in the world where Internet users challenged provider's storage of computer programs on computer hard drives of users who access websites affiliated with provider; the pleadings and evidence failed to prove that the provider's methods violated the SCA or the Wiretap Act).

\textsuperscript{152} Theofel v. Farey-Jones, 341 F.3d 978, 984–85 (9th Cir. 2003). The Ninth Circuit affirmed its interpretation of the SCA in Theofel v. Farey-Jones, 341 F.3d 978 (9th Cir. 2003), withdrawn by, 359 F.3d 1066 (9th Cir. 2004) (holding that an individual and his attorney violated federal electronic privacy and computer fraud statutes when they used a patently unlawful subpoena to gain access to email stored by a corporation's ISP—they were held civilly liable under the SCA because they procured the ISP's consent by exploiting a mistake of which they had constructive knowledge and access was not otherwise authorized).

\textsuperscript{153} United States v. Councilman, 373 F.3d 197, 204 (1st Cir. 2004) (quoting United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998)).

ECPA as a whole and implement a test to determine which title of the ECPA is applicable to the electronic communication at issue.

Courts should examine both titles of the ECPA, the Wiretap Act and the SCA, concurrently; this will help to prevent electronic communications from being acquired without consequence. It will also serve to further effectuate the purpose of the ECPA—to protect electronic communications. Furthermore, viewing the ECPA as one cohesive statute will force courts to determine the primary nature of the electronic communication at issue, either “in transit” or “in storage.”

In addition to viewing the ECPA as a whole, courts should employ a test to determine the primary nature of the electronic communication. Such a test would aid the courts in determining which title of the ECPA governs electronic communication that is both “in transit” and “in storage.” One such solution, which would not require amending the ECPA, would require courts to examine the nature of the electronic communication and classify it according to which state it is “predominantly in” at the time it is obtained or acquired. For example, perhaps what is occurring in Councilman is not temporary storage (as is included within the definition of electronic storage), but rather it is better characterized as storage necessary to facilitate the transmission of email. In this case, transmission should control because it is the primary and predominant action taking place. This “predominantly in” test would benefit courts by allowing them to more easily determine the nature of the electronic communication at issue and thus which title of the ECPA would be applicable in the situation.

Furthermore, this proposed test would be in accord with settled law, namely Steve Jackson Games. Steve Jackson Games has been criticized on the ground that the email at issue was obtained from the recipient’s inbox prior to being read and as such, the email was still in transmission because delivery was not completed. The proposed test, however, would rid the court’s decision of this criticism. Under the proposed test, the Fifth Circuit’s decision would be justified because at the time that the email messages were obtained, they were in the recipient’s inbox (they just had not been read); this state can be classified as predominately in storage.
Finally, it is interesting to note that the First Circuit has suggested in *Blumofe v. Pharmatrak, Inc.*\(^{155}\) that electronic communications are protected when they are in storage because by their nature they are in storage and transit simultaneously.\(^{156}\) The First Circuit noted in dicta that the Wiretap Act bans the interception of all electronic communications that are in transit, *whether or not they are stored temporarily.*\(^{157}\) This statement suggests that the First Circuit is at times confused and unclear as to its own position on what constitutes an "intercept" under the Wiretap Act.

**VII. Conclusion**

The Fifth Circuit noted that the Wiretap Act is "famous (if not infamous) for its lack of clarity."\(^{158}\) Courts have made reference to the notion that this is a problem that Congress, not the courts, should fix.\(^{159}\) Congress could amend the ECPA to clarify the provisions regarding interception of electronic communications and electronic storage.\(^{160}\) However, until then, courts should

---

\(^{155}\) 329 F.3d 9 (2003).

\(^{156}\) Here, the First Circuit stated in dicta that the Wiretap Act bans the interception of all electronic communications that are in transit, whether or not they are stored temporarily. The First Circuit found that a plaintiff must demonstrate five elements to make an interception claim under the ECPA. A plaintiff must show: "that a defendant (1) intentionally; (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept; (3) the contents of; (4) an electronic communication; (5) using a device." *Id.* at 18.

\(^{157}\) *Id.*

\(^{158}\) Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

\(^{159}\) United States v. Councilman, 373 F.3d 197, 204 (1st Cir. 2004) ("[T]he language may be out of step with the technological realities of computer crimes . . . it is not the province of this court to graft meaning onto the statute where Congress has spoken plainly."). The First Circuit stated it is the province of Congress to amend the Wiretap Act to extend to electronic communications the protections the Act affords wire and oral communications.

\(^{160}\) Since *Councilman*, the House of Representatives has introduced bills that would extend the protection of the Wiretap Act to electronic communication in electronic storage. On July 22, 2004, Representatives Inslee, Bartlett, Flake, and Delahunt introduced the E-mail Privacy Act of 2004, H.R. 4956, 108th Cong.
reflect, on whether it seems justifiable for electronic communications that are simultaneously "in transit" and "in storage" to come under the protections of either the Wiretap Act or the SCA or to fall outside of the protections of both? When asking this question, courts should keep in mind that the purpose of the ECPA is to expand privacy protections, previously applicable to only wire and oral communications, to include electronic communications.

If courts allow electronic communications that are simultaneously in transit and in storage to be acquired by ISPs without consequence, they are essentially reverting to the protections afforded electronic communications prior to the enactment of the ECPA—none. The First Circuit's narrow interpretation of the Wiretap Act in *Councilman* limits the privacy afforded electronic communications and disregards societal expectations of privacy.\(^{161}\) It is highly unlikely that Congress intended such a result.

---

\(^{161}\) Since one of the canons of statutory construction provides that courts should find a rational basis interpretation, the First Circuit should take the sure step of deciding that the undelivered email in *Councilman* was in fact "predominantly in" transit and intercepted as proscribed by the Wiretap Act.