United States Court of Appeals
For the First Circuit

No. 03-1383

UNITED STATES OF AMERICA,

Appellant,

v.

BRADFORD C. COUNCILMAN,

Defendant, Appellee.

APPEAL FROM THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MASSACHUSETTS

[Hon. Michael A. Ponsor, U.S. District Judge]

Before

Torruella, Circuit Judge,
Cyr, Senior Circuit Judge,
and Lipez, Circuit Judge.

Gary S. Katzmann, Assistant United States Attorney, with whom Michael J. Sullivan, United States Attorney, and Richard P. Salgado, Senior Counsel, Computer Crime and Intellectual Property Section, were on brief, for appellant.

Andrew Good, with whom Good & Cormier, was on brief, for appellee.

June 29, 2004

TORRUELLA, Circuit Judge. The United States appeals from the district court's dismissal of Count One of the Indictment against defendant Bradford C. Councilman ("defendant"). Count One charged defendant with conspiring to engage in conduct prohibited by various provisions of the Wiretap Act, 18 U.S.C. §§ 2510-2522, in violation of 18 U.S.C. § 371. We affirm.

I. Facts

Defendant was Vice-president of Interloc, Inc. ("Interloc"). Interloc's primary business was as an online rare and out-of-print book listing service. As part of its services, Interloc provided certain book dealer customers with an electronic mail ("e-mail") address and acted as the service provider. The dealer was provided with an e-mail account ending in "@Interloc.com".[1]

In May 1998, Alibris, a California corporation, acquired Interloc. Defendant was Vice-president, shareholder and employee of Interloc and Alibris. Among defendant's responsibilities was the management of the Internet Service Provider ("ISP") and the book dealer subscription list managed by Interloc.

---

[1] Interloc also did business under the name Valinet. Valinet functioned as an electronic service provider to the general public, not just bookdealers, for a monthly fee using the domain name @valinet.com. None of the e-mails at issue in this case were addressed by its sender to any addressee using the domain @valinet.com.

The parties stipulated to the following facts relevant to the transfer of electronic messages by the Interloc systems. An e-mail message, which is composed using an e-mail program, is transferred from one computer to another on its way to its final destination, the addressee. Building on the principle of store and forward, the message is handed to a Message Transfer Agent ("MTA") which stores the message locally. The message is routed through the network from one MTA to another until it reaches the recipient's mail server, which accepts it and stores it in a location accessible to the recipient. Once the e-mail is accessible to the recipient, final delivery has been completed. The final delivery process places the message into storage in a message store area. Often, a separate Mail Delivery Agent ("MDA") will be required to retrieve the e-mail from the MTA in order to make final delivery.

Interloc's computer facility used a program known as procmail (short for process mail) as its MDA. Procmail operates by scanning and sorting e-mail together with an MTA computer program known as "sendmail."

According to the Indictment, on or about January 1998, defendant directed Interloc employees to write computer code to intercept and copy all incoming communications from Amazon.com to subscriber dealers. The Interloc systems administrator wrote a revision to the mail processing code called procmail.rc ("the

procmail"), designed to intercept, copy, and store, all incoming messages from Amazon.com before they were delivered to the members' e-mail, and therefore, before the e-mail was read by the intended recipient. Defendant was charged with using the procmail to intercept thousands of messages. Defendant and other Interloc employees routinely read the e-mails sent to its members seeking to gain a commercial advantage.

The procmail was designed to work only within the confines of Interloc's computer. At all times that MTA sendmail and MDA procmail performed operations affecting the e-mail system, the messages existed in the random access memory (RAM) or in hard disks, or both, within Interloc's computer systems. Each of the e-mails at issue constituted an "electronic communication" within the meaning of 18 U.S.C. § 2510(12).

Count One of the Indictment charged defendant with a violation of 18 U.S.C. § 371 for conspiracy to violate 18 U.S.C. § 2511. Defendant allegedly conspired to intercept the electronic communications, to intentionally disclose the contents of the intercepted communications, in violation of 18 U.S.C. § 2511(1)(a), and to use the contents of the unlawfully obtained electronic communication, in violation of 18 U.S.C. § 2511(1)(c). Finally, the government alleged that defendant had conspired to cause a person to divulge the content of the communications while in transmission to persons other than the addressees of the

communications, in violation of 18 U.S.C. § 2511(3)(a).[2] The object of the conspiracy, according to the government, was to exploit the content of e-mail from Amazon.com, the Internet retailer, to dealers in order to develop a list of books, learn about competitors and attain a commercial advantage for Alibris and Interloc.[3]

Defendant moved to dismiss the Indictment for failure to state an offense under the Wiretap Act, as the e-mail interceptions at issue were in "electronic storage," as defined in 18 U.S.C. § 2510(17), and could not be intercepted as a matter of law. The district court did not initially grant the motion to dismiss but, upon further briefing by the parties, granted the motion and dismissed Count One. The district court found that the e-mails were in electronic storage and that, therefore, the Wiretap Act could not be violated because the requisite "interception" was lacking. United States v. Councilman, 245 F. Supp. 2d 319 (D. Mass. 2003).

---

[2] Count Two of the Indictment, which charged defendant with conspiracy to violate 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B), was dismissed at the request of the government after the district court granted defendant's motion to dismiss Count One.

[3] The stipulation signed by the parties also included a lengthy definition of the term e-mail. In this appeal, we are more concerned with the mechanism used to send and receive e-mail and therefore highlight those sections of the stipulation.

II. Analysis

A. The Wiretap Act

We review questions of statutory interpretation de novo. See United States v. Jones, 10 F.3d 901, 904 (1st Cir. 1993). The issue in this case is whether there was an "intercept" of a communication within the meaning of the Wiretap Act. In cases of statutory construction we begin with the language of the statute. See Hughes Aircraft Co. v. Jacobson, 525 U.S. 432, 438 (1999). We determine the meaning of a word from the context in which it is used. See Holloway v. United States, 526 U.S. 1, 6-7 (1999).

The Electronic Communications Privacy Act ("ECPA") amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968, commonly known as the federal wiretap law. See Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1999). The ECPA was divided into Title I, commonly known as the Wiretap Act, 18 U.S.C. §§ 2510-2522, and Title II, commonly known as the Stored Communications Act, 18 U.S.C. §§ 2701-2711.[4] The amendments provided for the protection of electronic communications along with oral and wire communications. See S. Rep. No. 99-541, at 11 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3565.

---

[4] The Wiretap Act and Stored Communications Act were amended again by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001). All references in this opinion are to the statute before it was amended.

We begin our analysis by highlighting the difference between the definitions of "wire communications" and "electronic communications" in the Wiretap Act, mindful that the communications at issue in this appeal are electronic in nature. Under 18 U.S.C. § 2510(1), a

> "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 furnished or operated by any person engaged in providing or operating such facilities . . . and such term includes any electronic storage of such communication. . . .

18 U.S.C. § 2510(1). By comparison, "'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." Id. at § 2510(12). No mention is made of electronic storage of electronic communications. See generally In re Hart, 328 F.3d 45, 49 (1st Cir. 2003)("[W]hen Congress includes a particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.").

"Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication

through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

The statute that defendant is charged with conspiring to violate, 18 U.S.C. § 2511, provides criminal penalties to be imposed on "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." 18 U.S.C. § 2511(1)(a).

Relying on the language of the statute and the decisions of our sister circuits, the district court held that Congress did not intend for the Wiretap Act's interception provisions to apply to communication in electronic storage. Councilman, 245 F. Supp. 2d at 321. The district court rejected "[t]he Government's position . . . that the Wiretap Act applies to interceptions that take place when the message . . . is 'in transit' or 'in process of delivery.'" Id. Relying on the definition of electronic storage, the district court held that no interception can occur while the e-mails are in electronic storage and therefore, without the requisite interception, the Wiretap Act could not be violated.

The scope of electronic communications that can theoretically be intercepted is obviously reduced when the definition does not include electronic storage of such communications, as is the case with wire communications. In addition, electronic storage includes a vast range of possible

situations including "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof . . . ." 18 U.S.C. § 2510(17)(A). The government argues that this section does not necessarily place the e-mails in question in this case outside the interception requirement of 18 U.S.C. § 2511(a).

The particular problem confronted in this case is what has been called the "contemporaneous" problem in the intercept requirement of the Wiretap Act. See In re Pharmatrak, 329 F.3d 9, 21-22 (1st Cir. 2003)(because the statute was written before the widespread use of the Internet and other media prior opinions may not be helpful in addressing current problems). The government argues that given the particular nature of electronic communications and the mechanisms used to retrieve them, 18 U.S.C. § 2511(a) is a proper foundation for Count One of the Indictment. In addition, the government argues, cases from other circuits are distinguishable on their facts because none used the procmail at issue in this case.[5] We have commented on the issue presented in this case, see Pharmatrak, 329 F.3d at 21-22, but have not resolved it.[6]

---

[5] The government refers to the procmail as an e-mail syphon.

[6] Pharmatrak did not resolve the issue because the interception there was at the point where communications were being sent through a wire to the website. The messages were not placed in any type of storage before their interception, therefore skirting the "contemporaneous" problem.

The first case to address the issue of unlawful intercept in the context of electronic communications is Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994). There, the plaintiff company sued the Secret Service because the agency had seized a computer used to operate a bulletin board system, but which also contained private, unretrieved electronic mail. Id. at 459. The plaintiff provided its customers with the ability to send and retrieve e-mail, which was stored on the company's hard disk drive temporarily, until the recipient retrieved the e-mail. Id. at 458. After seizing the computer, the Secret Service allegedly opened the private e-mails, read them and deleted them. The company sued, alleging, inter alia, a violation of the Wiretap Act. Id. at 459-60.

The Fifth Circuit held that the seizure of sent but unretrieved e-mail did not constitute an intercept for purposes of 18 U.S.C. § 2511(1)(a). See Steve Jackson Games, 36 F.3d at 461-62. In reaching that conclusion, it relied on the difference in the definitions of electronic and wire communication and the definition of electronic storage. "Congress' use of the word 'transfer' in the definition of 'electronic communication,' and its omission in that definition of the phrase 'any electronic storage of such communication' (part of the definition of 'wire communication') reflects that Congress did not intend for 'intercept' to apply to 'electronic communications' when those

communications are in 'electronic storage.'" Id. (footnote omitted); see also Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003) (adopting the reasoning in Steve Jackson Games as to the meaning of intercept under the relevant version of the Wiretap Act).

In contrast, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003), concerned a plaintiff, an employee of Hawaiian Airlines, who operated a secure website which posted criticism of his employer. A vice-president of the airline obtained permission from authorized users to view the website. Plaintiff sued, alleging, inter alia, that defendant had violated the Wiretap Act by violating the terms of use of the website and entering a secure website under false pretenses.

The Ninth Circuit, after granting panel rehearing, reversed its earlier position that the electronic communications were covered under the Wiretap Act. It did so because, in its view, the conduct of the defendant did not constitute an intercept as that term is defined. Konop, 302 F.3d at 876. Relying on Steve Jackson Games, it 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 in electronic storage." Id. at 878. In doing so, it rejected the position the government takes in this case, that, given the nature of e-mail, the Wiretap Act must apply

to en route storage. Id. at 879 n.6. "While this argument is not without appeal, the language and structure of the [Act] demonstrate that Congress considered and rejected this argument." Id. The court relied, as did the district court in this case, on the expansive definition of the term "electronic storage" in 18 U.S.C. § 2510(17)(A). The dismissal of the Wiretap Act claim was affirmed.

The government is correct that the electronic communications at issue here were acquired in a different manner than in Steve Jackson Games and Konop. Defendant's procmail operated to obtain the e-mails before they were received by its intended recipients. While the e-mail in Steve Jackson Games was retrieved from storage in a computer and the website in Konop was accessed under false pretenses, the e-mails in this case were accessed by the procmail as they were being transmitted and in real time. However, the presence of the words "any temporary, intermediate storage" in 18 U.S.C. § 2510(17) controls. On the facts of this case, it is clear that the electronic communications in this case were in a form of electronic storage. It may well be that the protections of the Wiretap Act have been eviscerated as technology advances. See United States v. Steiger, 318 F.3d 1039, 1047-51 (11th Cir. 2003) (holding intercept did not occur because there was no contemporaneous acquisition but commenting that under the narrow reading of the statute few seizures will constitute

interceptions under Wiretap Act). As the stipulation reached by the parties states, "[a]t all times that sendmail and procmail performed operations affecting the email messages at issue, the messages existed in the random access memory (RAM) or in hard disks, or both, within Interloc's computer system." When defendant obtained the e-mails, they were in temporary storage in Interloc's computer systems. There was also a stipulation that "[n]either sendmail nor procmail performed functions that affected the emails in issue while the emails were in transmission through wires or cables between computers." This fact places the messages outside the scope of 18 U.S.C. § 2511(a), and into temporary electronic storage under 18 U.S.C. § 2510 (17)(A). Accord Steiger, 318 F.3d at 1049; Konop, 302 F.3d at 878; Steve Jackson Games, 36 F.3d at 462; see also United States v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997) (holding that for Wiretap Act provisions to be violated as to electronic communications contemporaneous acquisition is necessary); United States v. Reyes, 922 F. Supp. 818, 836 (S.D.N.Y. 1996) (same).

The government argues, and the dissent is persuaded by this argument, that the legislative history of the statute demonstrates that if an electronic communication is obtained while it is simultaneously in transmission and in storage, then an intercept occurs. Notwithstanding the fact that we find the language of the statute unambiguous, exploring this contention

merely confirms our position as to the meaning of the statute. The government points to dicta in Pharmatrak as supporting the conclusion that electronic communications are protected when they are in storage, because by their nature, they exist in storage and transit at the same time.

> [T]he storage-transit dichotomy adopted by earlier courts may be less than apt to address current problems. As one court recently observed, "[t]echnology has, to some extent, overtaken language. Traveling the internet, electronic communications are often -- perhaps constantly -- both 'in transit' and 'in storage' simultaneously, a linguistic but not a technological paradox."

329 F.3d at 21-22 (quoting Councilman, 245 F. Supp. 2d at 321). However, the legislative history of the Act clearly states that the definition of intercept was not altered by the amendments. See S. Rep. No. 99-541, at 12, reprinted in 1986 U.S.C.C.A.N. at 3566 (stating that "[t]he definition of 'intercept' under current law is retained with respect to wire and oral communications except that the term 'or other' is inserted after 'aural'"). Even assuming arguendo that we should look outside the text, the government's arguments based on the legislative history are unavailing.

The Wiretap Act's purpose was, and continues to be, to protect the privacy of communications. We believe that the language of the statute makes clear that Congress meant to give lesser protection to electronic communications than wire and oral communications. Moreover, at this juncture, much of the protection

may have been eviscerated by the realities of modern technology. We observe, as most courts have, that the language may be out of step with the technological realities of computer crimes. However, it is not the province of this court to graft meaning onto the statute where Congress has spoken plainly.[7] We therefore affirm the district court's dismissal of Count One of the Indictment on the premise that no intercept occurred in this case, and therefore, the Wiretap Act could not be violated.

B. The Stored Communications Act

Defendant also argues that his conduct was lawful under Title II of the ECPA, or the Stored Communications Act, 18 U.S.C. § 2701 et seq., and therefore outside the criminal provisions of the Wiretap Act. Specifically he relies on the provider exceptions, 18 U.S.C. § 2701(c)(1). Given our reading of the Wiretap Act, we need not comment on this argument. We note, however, that the intersection of the Wiretap Act and the Stored Communications Act "is a complex, often convoluted, area of the law." United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998). Defendant's argument takes us beyond the charges in the Indictment. Therefore, we need not stray beyond the text of the Wiretap Act

[7] In fact, defendant is correct to make an argument, on due process grounds, that he is entitled to the benefit of any ambiguity in the statute. While we find there is no ambiguity in Congress's language, in a criminal case we have the constitutional obligation to define language narrowly. See, e.g., United States v. Colón-Ortiz, 866 F.2d 6, 8 (1st Cir. 1989).

into the Stored Communications Act because the government sought to indict defendant only for conspiracy to violate Title I, 18 U.S.C. § 2511(a).

III. Conclusion

For the reasons stated above, the district court's order dismissing Count One is **affirmed**.

"Dissenting Opinion follows"

LIPEZ, Circuit Judge (Dissenting). Unlike my colleagues, I believe that the district court erred in dismissing the indictment against Defendant-Appellee Bradford Councilman for violating Title I of the Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986). To explain my disagreement, I will present some background information on the technology at issue and Congress's passage of the ECPA. That background is critical to an understanding of the issue before us. I will then set forth Councilman's arguments as I understand them and explain why I find them unpersuasive. I will then address the government's persuasive arguments. In discussing this material, I will also respond to the reasoning of the district court and my colleagues.

I. The Technology

The Internet consists of a network of inter-connected computers in which data are broken down into small, individual packets and forwarded from one computer to another until they reach their destinations. 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). Each service on the Internet--e.g. e-mail, web hosting, and instant messaging--has its own protocol for using those packets of data to transmit information from one place to another. I will focus solely on the e-mail protocol. After a user composes a message in an e-mail program, a mail transfer agent

("MTA") formats that message and sends it to another program that "packetizes it" and sends those packets out to the Internet. Computers on the network then pass the packets from one to another; each computer along the route stores the packets in memory, retrieves the address of their destination, and then determines where to send it next based on the packet's destination. At various points the packets are reassembled to form the original e-mail message, copied, and then repacketized for the next leg of the journey. See J. Klensin, RFC 2821 - Simple Mail Transfer Protocol, available at http://www.faqs.org/rfcs/rfc2821.html (last accessed May 19, 2004) (containing the standard for the Simple Mail Transport Protocol). These intermediate computers occasionally retain backup copies of the e-mails that they forward and then delete those backups a short time later. The method of transmission is commonly called "store and forward" delivery.

Once all the packets reach the recipient's mail server, they are reassembled to form the e-mail message. A mail user agent ("MUA"), which in Councilman's case was a program called "Procmail," then determines which user should receive the e-mail and places the message in that user's mailbox. The MUA is controlled by programs called "recipe files." These recipe files can be used in a variety of ways and can, for example, instruct the MUA to deposit mail addressed to one address into another user's mailbox (i.e., to send mail addressed to "help" to the tech support

department), to reject mail from certain addresses, or to make copies of certain messages. Once the messages are deposited in a mailbox, the end user simply needs to use an e-mail program to retrieve and read that message. Councilman wrote a recipe file for his MUA that caused all of the messages from Amazon.com to be copied while the MUA was in the process of placing that message into the recipient's mailbox, and to place these copies into his own personal box.

II. The Legislative Context

Congress passed the 1968 Wiretap Act to "protect[] the privacy of wire and oral communications, and [to] delineat[e] on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." Gelbard v. United States, 408 U.S. 41, 48 (1972) (quoting S. Rep. No. 90-1097, at 66 (1968), reprinted in 1968 U.S.C.C.A.N. 2153, 2153). By the mid-1980s, however, technology had outpaced the privacy protections in the Act, creating uncertainty and gaps in its coverage. As one member of the House Judiciary Committee lamented:

> [I]n the almost 20 years since Congress last addressed the issue of privacy of communications in a comprehensive fashion, the technologies of communication and interception have changed dramatically. Today we have large-scale electronic mail operations . . . and a dazzling array of digitized information networks which were little more than concepts two decades ago. These new modes of communication have outstripped the legal

> protection provided under statutory definitions bound by old technologies.

Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Adminstration of Justice of the House Comm. on the Judiciary, 99th Cong. 1 (1985-1986) (statement of Chairman Kastenmeier); See also id. at 3 ("[T]he American people and American businesses are no longer assured that the law protects their right to communicate privately.") (Statement of Sen. Leahy). Congress passed the ECPA to remedy these perceived weaknesses and to update and expand the privacy protections in the 1968 Act. See Sen. Rep. No. 99-541, at 1 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3555 ("The bill amends the 1968 law to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.").

Title I of the new act amended the 1968 Wiretap Act and added new protections for electronic and digital technologies. Section 101(c)(1)(A) added "electronic communications" to the existing prohibitions against intercepting wire--which are essentially telephone calls--and oral communications. As the House report made clear, Congress intended to give the term "electronic communication" a broad definition: "As a rule, a communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterized as one containing the human voice (carried in part by wire)." H.R. Rep. No. 99-647, at 35. Section

101(a)(3) added "or other" to the definition of "intercept," which had previously only referred to the "aural acquisition of the contents of any . . . communication."[8] Also relevant to this case, albeit not at issue here, Section 101(c)(7) removed a phrase in the Wiretap Act that limited the scope of the Act to communications transmitted on common carriers. This amendment expanded the reach of the Act's protections to private telephone and computer

---

[8] Prior to the 1986 amendments, the Wiretap Act's definition of "wire communication" read:

> "[W]ire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

The post-ECPA version of that definition read:

> "[W]ire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication.

Congress deleted the phrase "and such term includes any electronic storage of such communication" in 2001.

networks, including internal office networks, and cellular phones. The amended Wiretap Act now reads, in pertinent part: "[A]ny person who intentionally intercepts, endeavors to intercept, or procures any person to intercept or endeavor to intercept, any wire, oral or electronic communication . . . shall be punished . . . ." 18 U.S.C. § 2511(1).

Congress also recognized that, with the rise of remote computing operations and large databanks of stored electronic communications, the threats to individual privacy extended well beyond the bounds of the Wiretap Act's prohibition against the "interception" of communications. These stored communications--including stored e-mail messages, stored financial transactions, stored medical records, and stored pager messages--were not protected by the Wiretap Act, presumably because the Act had been interpreted to only prohibit "the contemporaneous acquisition of [a] communication." See United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976). Therefore, Congress concluded that "the information [in these communications] may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties." Sen. Rep. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557; see also United States Congress, Office of Technology Assessment, Electronic Surveillance and Civil Liberties 48-50 (1985) (theorizing that communications service providers and banks could disclose private

information about their customers without federal liability and law enforcement agents could seize these private communications with only a modicum of procedural protections).

Congress added Title II to the ECPA to halt these potential intrusions on individual privacy. This title, which is commonly referred to as the Stored Communications Act, established new punishments for any person who "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 . . . ." 18 U.S.C. § 2701(a).

The privacy protections established by the Stored Communications Act were intended to apply to two categories of communications: "those associated with transmission and incident thereto" and those of "a back-up variety." H.R. Rep. No. 99-647, at 68. The first category refers to temporary storage such as when a message sits in an e-mail user's mailbox after transmission but prior to the user retrieving the message from the mail server. Importantly, however, this category does not include messages that are still in transmission, which remain covered by the Wiretap Act. Id. at 65 (stating that the Wiretap Act "prohibits . . . a provider from divulging the contents of a communication while it is in transmission."). The second category includes communications that

are retained on a server for administrative and billing purposes. Communications service providers could use stored messages in this category to restore a user's data in the event of a system crash or to recover accidentally-deleted messages.

Defendant-Appellee Bradford Councilman was indicted on July 11, 2001 for violating Title I of the ECPA, the Wiretap Act, but was not charged with violating Title II, the Stored Communications Act. Determining the legality of this indictment requires us to explore the dividing line between these two titles. Councilman claims that the e-mails at issue were stored communications when they were being processed for delivery in his company's computers, and, therefore, they were not the type of "evanescent" transmissions, i.e., telephone calls traveling through a wire, that the Wiretap Act addresses.[9] Under his approach, an 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. According to Councilman:

> The reason that the stored v. evanescent distinction is a key determinant of the extent of privacy protection afforded by the ECPA to both wire and electronic communications is simply that, because of their lasting nature, stored communications are inherently more vulnerable to intrusion than evanescent

[9] Webster's defines "evanescent" as "vanishing; fading away; fleeting." Random House Webster's Unabridged Dictionary 670 (2d ed. 1997).

> communications, which must be intruded upon simultaneously with the communication, or not at all.

The government focuses on the temporal nature of Councilman's actions and argues that he violated the Wiretap Act because he copied the e-mails "contemporaneously with their transmission." In other words, he copied them in real time while they were in the process of being delivered. Under its view, an intercept is subject to the Wiretap Act between the time that the author presses the "send" button and the time that the message arrives in the recipient's e-mail box. Accordingly, the Wiretap Act would apply to messages that are intercepted contemporaneously with their transmission and the Stored Communications Act would apply to messages that are accessed non-contemporaneously with transmission.

As I discuss in greater detail in Section V, infra, the line that we draw in this case will have far-reaching effects on personal privacy and security. Congress concluded that stored communications, while requiring protection, require fewer privacy protections than those in transit. Therefore, the Wiretap Act includes significant procedural protections which go beyond the requirements of the Fourth Amendment itself and which are not applicable to the Stored Communications Act. First, officers may only obtain wiretap orders for investigations involving federal felonies. See 18 U.S.C. § 2516(3). Second, in addition to

demonstrating that they have probable cause, the officers must provide specific information regarding, inter alia, the types of communications that would likely be intercepted, the individuals whose conversations would be intercepted, the steps that the agents took to avoid having to rely on a wiretap, and the steps that they would take to avoid intercepting more information than is necessary. 18 U.S.C. §§ 2518(1)-(4). Third, unless the court grants a special extension, the wiretap may only last for the shorter of thirty days or as long as is necessary to obtain the necessary evidence. Id. § 2518(5). Fourth, the court may require the Government to produce regular reports on the progress of its wiretaps and to keep the tapes and transcripts of those wiretaps under seal. Id. §§ 2518(6) & 8(a). Fifth, the court must notify the target of the wiretap application--within a reasonable time--that their communications may have been intercepted. Id. § 2518 (8)(d). Finally, if the officers violate any portion of these rules, the evidence obtained through the wiretap is automatically suppressed, even if the Government's actions did not violate the Fourth Amendment. Id. § 2515.

The Stored Communications Act does not contain any of the Wiretap Act's special protections. A federal law enforcement agent could obtain access to such communications simply by obtaining a

warrant. 18 U.S.C. § 2703(a).[10] The target of the investigation does not need to be informed that the government accessed his or her communications, id. at § 2703(b)(1)(A), and a defendant does not have the right, outside of the Fourth Amendment, to seek to suppress communications that were obtained in violation of the Stored Communications Act.

It is also easier for private actors to access private messages under the Stored Communications Act. Section 2702(a) exempts, inter alia, "conduct authorized by the person or entity providing a wire or electronic communications service" from the prohibition against unauthorized access. Thus, a private actor like Councilman may open a user's files and may read the e-mails that are stored in that user's mailbox. But see 18 U.S.C. § 2702

---

[10] According to the Stored Communications Act:

> A Governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal rules of Criminal Procedure . . . or equivalent State warrant.

18 U.S.C. § 2703(a). See also id. § 2703(b)(1) ("A governmental entity may require a provider of remote computing service to disclose the contents of any [stored e-mail] without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . or equivalent State warrant . . . .").

(stating that service providers may not, with certain objections, disclose stored communications that they access). The Wiretap Act does not include any such broad exemption.[11]

III. Councilman's Arguments

A. The Plain Text

Councilman's primary argument, which was dispositive with the district court and now with my colleagues, is that the plain text of the ECPA exempts electronic communications that are in storage from the purview of the Wiretap Act. In brief, he argues that Congress included the term "electronic storage" in the ECPA's definition of "wire communication" but failed to do so in the definition of "electronic communication."[12] That omission,

---

[11] As noted, Title I of the Electronic Communications Privacy Act amended the 1968 Wiretap Act. From this point forward, when I refer to the "Wiretap Act," I mean the 1968 Wiretap Act as amended by Title I of the ECPA. I will refer to Title II of the ECPA simply as the Stored Communications Act.

[12] "Electronic communication" is defined 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 that affects interstate or foreign commerce, but does not include--
>
> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

according to Councilman, indicates that Congress intended to exclude communications that are in storage from the definition of "electronic communication" and, hence, from the scope of the Wiretap Act. Moreover, Congress defined the term "electronic storage" expansively to include "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17). See United States v. Councilman, 245 F. Supp. 2d. 319, 320 (D. Mass. 2003) (describing this definition as "extraordinarily--indeed, almost breathtakingly broad"). Since the parties stipulated that the e-mails in this case were "in the random access memory (RAM) or in the hard disks, or both, within [Councilman's company's] computer system" at the time of the interception, those e-mails fall under the statutory definition of "in storage."

As so often happens under close scrutiny, the plain text is not so plain. There is no explicit statement from Congress that it intended to exclude communications that are in storage from the definition of "electronic communication," and, hence, from, the scope of the Wiretap Act. Councilman, without acknowledging it, looks beyond the face of the statute and makes a non-textual, inferential leap. He infers that Congress intended to exclude all communications that are in storage from the definition of "electronic communication," regardless of whether they are in the

---

18 U.S.C. § 2510(12).

process of being delivered, simply because it did not include the term "electronic storage" in that definition. This inferential leap is not a plain text reading of the statute.[13]

As I discuss in greater detail in Section IV, this inferential leap ignores the rationale behind Congress's inclusion of electronic storage in the definition of "wire communication." Recognizing that telephone calls would no longer be protected by the Wiretap Act after they were stored in voicemail, Congress wanted to expand the scope of the Wiretap Act to embrace these stored communications. Although this decision might indicate that Congress did not intend to use the Wiretap Act to protect e-mails after they have been delivered, it says nothing about Congressional intent regarding e-mails that are still in transmission. Furthermore, my colleagues use that maxim to impute meaning to the statute that the legislative history does not support. Congress

---

[13] My colleagues quote the maxim: "[W]hen Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion," see, e.g., In re Hart, 328 F.3d 45, 49 (1st Cir. 2003). This maxim is a canon of construction, see, e.g., Trenkler v. United States, 268 F.3d 16, 23 (1st Cir. 2001) (characterizing the maxim as a canon of construction). This reliance on the canon to support the inferential leap belies the availability of a plain text argument. Cf. Springer v. Government of Philippine Islands, 277 U.S. 189, 206 (1928) ("The general rule that the expression of one thing is the exclusion of others is subject to exceptions. Like other canons of statutory construction, it is only an aid in the ascertainment of the meaning of the law, and must yield whenever a contrary intention on the part of the lawmaker is apparent.").

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. We should not misconstrue this easily understood inclusion of post-delivery voicemail storage as indicating an unstated intention to exclude emails in transmission from the scope of the Wiretap Act. See Clay v. United States, 537 U.S. 522, 523 (2003) (rejecting the notion that Congress's failure to use a particular term in a definition must have been deliberate when "one can readily comprehend why Congress might have found it appropriate to spell out the meaning of "final" in [one section] but not in [another]").

Moreover, Councilman ignores an important rule of statutory interpretation: "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." Andrus v. Glover Constr. Co., 446 U.S. 608, 616-17 (1980). From the prohibition that, "No person shall intentionally intercept an electronic communication," Congress specifically excluded four categories of communications: 1) wire and oral communications; 2) communications made through tone-only paging devices; 3) communications from tracking devices; 4) electronic funds transfer information stored by a financial institution. 18 U.S.C. § 2510(12). Councilman's approach would engraft an additional exclusion onto this list: "any communication

in electronic storage." A commonsensical reading of the statute and a respect for our precedents preclude the implication of such an exclusion without additional support in the legislative record. See also American Tobacco Co. v. Patterson, 456 U.S. 63, 71 (1982) ("Statutes should be interpreted to avoid untenable distinctions and unreasonable results whenever possible.").

In short, the plain text of the ECPA does not clearly address the issue of whether a communication is still considered an electronic communication when it is in electronic storage during transmission. Given this ambiguity, I turn to Councilman's arguments regarding Congressional intent and legislative history.

B. Congressional Intent and Legislative History

Without yielding on his plain meaning arguments, Councilman claims that Congress intended to accord greater protection to wire communications than to electronic communications. Noting that § 2510(1) expanded the Wiretap Act's coverage to stored voicemails, he sees that provision as indicative of a Congressional intent to provide a lower degree of protection to e-mails that are stored while they are being delivered. Without citing any relevant evidence in the Congressional Record, Councilman theorizes that Congress decided to provide greater protections to wire communications because participants in telephone calls may have a greater expectation of privacy than participants in e-mail exchanges. As he puts it: "In Congress'

view, a lesser, non-constitutional degree of expectation of privacy can or should attach to forms of communication that are not evanescent, but rather are inherently subject to being stored by non-parties to the communication."

The legislative history does not support this assertion. To the contrary, the legislative history demonstrates that Congress was deeply concerned about the emerging threats to privacy and the failure of existing legal protections to cope with those threats. See In re Pharmatrak, 329 F.3d 9, 18 (1st Cir. 2003) ("The paramount objective of the Wiretap Act is to protect effectively the privacy of communications."). Councilman's approach, which would apply the Stored Communications Act to e-mails during delivery, is undermined--not supported--by legislative history demonstrating that the purpose of the ECPA was to provide greater protections to electronic communications under the Wiretap Act.

Congress requested a report from the Office of Technology Assessment (OTA) shortly before undertaking its consideration of the Wiretap Act in 1983. The report, Electronic Surveillance and Civil Liberties, used stark language to describe the existing privacy protections:

> In the last 20 years, there has been a virtual revolution in the technology relevant to electronic surveillance. Advances in electronics, semiconductors, computers, imaging, databases and related technologies have greatly increased the technical options for surveillance activities . . . The existing statutory framework and jurisdictional

> interpretations thereof do not adequately cover new electronic surveillance applications.

The report then identified threats associated with five different types of surveillance--telephone, e-mail, electronic physical, electronic visual, and database--and suggested statutory reforms to protect individual privacy from those threats. This report was important in shaping the ECPA. Congress repeatedly cited it during its deliberations.

The stated purpose of the ECPA was 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." S. Rep. No. 99-541, at 1 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3555. Congress repeatedly stressed the need for new protections for both telephone and electronic communications. See, e.g., id. at 5, reprinted in 1986 U.S.C.A.A.N. 3555, 3559 ("[T]here are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by . . . new forms of telecommunications and computer technology."); Id. at 4 (observing that existing protections for e-mail were "'weak, ambiguous, or non-existent' and that 'electronic mail remains legally as well as technically vulnerable to unauthorized surveillance.'") (quoting Office of Technology Assessment, Electronic Surveillance and Civil Liberties 45 (1985)); Id. at 3

("Electronic hardware making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others are readily available in the American market today."); H.R. Rep. No. 99-647, at 34 (1986) (characterizing electronic mail as "one of the most popular new computer services" and stating that through the protections in the ECPA "electronic mail will be provided with protection against interception").

Indeed, while the legislative history includes a few statements regarding the balance between law enforcement and individual liberty, the perceived need to protect privacy was the overarching motivation for the bill. According to the Senate Report:

> [T]he law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

S. Rep. No. 99-541, at 5 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3559 (1986). Congress did not express any desire to accord less protection to electronic communications. In fact, one of the authors of the ECPA said that the legislation constituted

> a recognition that what is being protected is the sanctity and privacy of the communication. We should not attempt to discriminate for or against certain methods of communication, unless there is a compelling case that all

> parties to the communication want the message accessible to the public.

132 Cong. Rec. H4039 (Statement of Rep. Kastenmeier).

Oddly, Councilman relies on legislative history that actually undercuts his position when he quotes from the Senate Report:

> Nevertheless, because [copies of e-mails retained on mail servers are] subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection. Thus, the information may be open to possible wrongful use and disclosure by law enforcement authorities as well as unauthorized private parties. The provider of these services can do little under the current law to resist unauthorized access to communications.

S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557 (1986). Rather than reflecting Congress's comfort with less privacy protection for electronic communications, the Senate report cited the lack of constitutional protection as a justification for creating greater, not lesser, statutory protections for e-mails. There is no support in the legislative record for the proposition that Congress intended to apply the Stored Communications Act to e-mails that are stored during transmission.

C. Other Precedents

Councilman's effort to support his plain text argument with references to precedents outside of this circuit is also unavailing. First, he cites Steve Jackson Games, Inc. v. United

States Secret Service, 36 F.3d 457 (5th Cir. 1994) in which the Fifth Circuit considered a complaint against federal officers for seizing a computer bulletin board system (BBS) that contained unread e-mails. The court rejected the plaintiffs' claim that this seizure constituted a violation of the Wiretap Act, holding that the plain language of the statute--specifically, the omission of the term "electronic storage" from the definition of "electronic communication"--"reflects that Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'" Since the messages were being stored on the seized server, the Wiretap Act did not apply. Id. at 462.

Councilman fails to account for the context of this case. The Steve Jackson court was faced with the question of whether a non-contemporaneous communication could be "intercepted" under the Wiretap Act; it answered that question in the negative. That holding is fully in line with the Government's position in this case. In fact, the court went out of its way to note that "intercept" was defined as contemporaneous in the context of an aural communication under the old Wiretap Act, and that Congress retained this definition when it passed the ECPA. Steve Jackson Games, 36 F.3d at 461. See also Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) (citing Steve Jackson Games and concluding that "[e]very circuit court to have considered the

matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission."). The type of temporary storage during delivery that is at issue in this case is irrelevant to the post-transmission storage that was at issue in Steve Jackson Games.

Councilman and the district court also cite Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 n.6 (9th Cir. 2002), a case in which the court rejected an attempt by a civil plaintiff to broaden the scope of the Wiretap Act to encompass communications stored on a website. In a footnote, the Konop court noted that "[t]he dissent, amici, and several law review articles argue that the term 'intercept' must apply to electronic communications in storage because storage is a necessary incident to the transmission of electronic communications," and "if the term 'intercept' does not apply to the en route storage of electronic communications, the Wiretap Act's prohibition against 'intercepting' electronic communications would have virtually no effect." Although the court found these argument appealing, it held that "the language and structure of the ECPA demonstrate that Congress considered and rejected this argument," and that the Act's broad definition of the term "electronic storage" belied the plaintiff's interpretation of the Wiretap Act. Id.

Again, context is important. The Konop court faced the question of whether a company could be held liable for accessing

the employees' private secure website without authorization. Since the data in a website are static and the Act requires interception contemporaneous with a communication, id. at 878-79, it held that data stored in a website cannot be considered to be illegally intercepted under the Wiretap act by unauthorized access to that website. It did not hold that electronic communications lose the protection of the Wiretap Act as soon as they reach a computer.[14] Like the Steve Jackson court, the Konop court reiterated the view that an intercept under the Wiretap Act is defined as an acquisition contemporaneous with transmission. Id. at 878.

Finally, Councilman briefly cites to dicta in United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003), which stated: "'There is only a narrow window during which an E-mail interception may occur--the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command.'" Id. at 1050 (quoting Jarrod J. White, E-Mail @Work.com: Employer Monitoring of Employee E- Mail, 48 Ala. L. Rev. 1079, 1083 (1997)). Councilman failed to note that the article

---

[14] Councilman also argues that the government should be judicially estopped from asserting that he violated the Wiretap Act since it argued in favor of the holdings in Steve Jackson Games and Konop. This argument is misguided. In fact, the government has consistently argued that a communication needs to be intercepted contemporaneously with transmission to violate the Wiretap Act. See InterGen N.V. v. Grina, 344 F.3d 134, 144 (1st Cir. 2003) ("[T]he doctrine of judicial estoppel prevents a litigant from pressing a claim that is inconsistent with a position taken by that litigant either in a prior legal proceeding or in an earlier phase of the same legal proceeding.") (emphasis added).

quoted by the Eleventh Circuit was discussing the impact of the Steve Jackson decision on employers' obligations regarding e-mail. Like the Steve Jackson court, the article did not discuss storage during transmission, and it appears that the "temporary location" referred to in the quoted sentence was an employee's e-mailbox. Even if the language quoted by the Steiger court was part of its holding, it would not support Councilman's interpretation of the ECPA.

D. Our Precedent

Apparently recognizing that his narrow definition of the Wiretap Act contradicts our Pharmatrak decision, Councilman attempts to distinguish that case from this one by pointing out that the defendant in that case did not operate an electronic communication service, and by claiming that the communication in that case was not "in storage." The first distinction is irrelevant. While such operators have limited immunity under the Stored Communications Act, see 18 U.S.C. § 2701(c)(1), the Wiretap Act does not shield operators from liability for the type of conduct at issue in this case.

The second distinction contradicts the rest of Councilman's argument. The defendant company in Pharmatrak installed software on Internet users' computers to track the websites that they visited and to log the information that they sent to those websites. The program recorded this information in

real time and sent that data to one of Pharmatrak's computers for processing. The captured information would qualify as being "in storage" under Councilman's definition: it was either stored in RAM or on a user's computer hard drive when the program accessed it. We dismissed this distinction, however, focusing our analysis on the temporal nature of the interception, and holding that the defendant violated the Wiretap Act because "[t]he acquisition by Pharmatrak was contemporaneous with its transmission by the internet users." Id. at 22.[15]

Although we discussed the ongoing debate about how strictly courts should construe the contemporaneity requirement, we concluded that we did not have to resolve that issue because "[e]ven those courts that narrowly read 'interception' would find that Pharmatrak's acquisition was an interception." Id. We quoted the Steiger court:

> [U]nder the narrow reading of the Wiretap Act we adopt . . ., very few seizures of electronic communications from computers will constitute 'interceptions.' . . . 'Therefore, unless some type of automatic routing software

---

[15] My colleagues attempt to distinguish the interception in Pharmatrak from the interception here by claiming that the communications in Pharmatrak "were not placed in any type of storage before their interception." In fact, the Pharmatrak defendant's Java/Javascript programs recorded the URLs that the users visited, which means that they copied the users' web commands before those commands were sent over the Internet. The web commands were in the same type of temporary, intermediate, and incidental storage that the e-mails at issue in this case were in when they were intercepted; therefore, our conclusion that there was an interception in Pharmatrak should control our analysis here.

> is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-Mail within the prohibition of [the Wiretap Act] is virtually impossible.'

Id. (quoting United States v. Steiger, 318 F.3d at 1050 (alterations in original). We then noted that Pharmatrak's program would qualify under the Steiger definition because it effectively was an automatic routing program. Id. Much like the data logging program there, the Procmail recipe file here acted as an automatic routing program. It analyzed all of the e-mails sent to Councilman's mail server in real time and copied the relevant ones while they were being delivered.

E. Vagueness

Finally, Councilman claims that even if his conduct violated the Wiretap Act, the district court correctly dismissed his indictment on vagueness grounds because the government's interpretation of the act "criminalize[s] a broad variety of conduct that is widely and reasonably understood to be lawful."

The vagueness doctrine reflects the fundamental notion that "due process requires that criminal statutes put individuals on sufficient notice as to whether their contemplated conduct is prohibited." Sabetti v. DiPaolo, 16 F.3d 16, 17 (1st Cir. 1994) (quoting United States v. Colón-Ortiz, 866 F.2d 6, 8 (1st Cir. 1989)). This standard is violated only when "a person of ordinary intelligence examining [only] the language of the statute would be

in some way surprised that it prohibited the conduct in question." Id. (internal quotations omitted). Mere textual ambiguity is not sufficient: "If run-of-the-mill statutory ambiguities were enough to violate the Constitution, no court could ever clarify statutes through judicial interpretation." Id. at 18.

The Wiretap Act explicitly states that "any person who intentionally intercepts . . . [any] electronic communication . . . shall be punished . . . ." As the Government aptly observes in its brief:

> There is nothing about defendant's conduct that the average person would generally consider innocent. There is nothing on the face of the Wiretap Act that would lull a person of average intelligence into believing that an electronic communications provider may intercept electronic mail and disclose its contents for commercial purposes.

Although Councilman claims that his scheme to copy and review incoming e-mails was no different than the monitoring and junk e-mail filtering that employers, schools, and other institutions routinely implement, he fails to note that these entities do so with notice and the consent of their users, and, therefore, that their conduct is not illegal. See 18 U.S.C. § 2511(2)(d) ("It shall not be unlawful under this chapter for a person . . . to intercept a wire, oral, or electronic communication . . . where one of the parties to the communication has given prior consent to such interception . . . ."). There is nothing vague about the Wiretap

Act, and Councilman should not have been surprised that his conduct constituted an illegal interception.

IV. The Government's View

According to the Government's view of the ECPA, "an 'intercept' occurs [and the Wiretap Act applies] when one acquires an electronic communication contemporaneous with its transmission." It is irrelevant that the transmission may have been in electronic storage at the time of the acquisition. In my view, this interpretation of the Act is consistent with Congressional intent, precedent, and the realities of electronic communication systems.

The district court seemed to agree with one predicate of the Government's argument when it acknowledged that "technology has, to some extent, overtaken language" and that "[t]raveling the Internet, electronic communications are often--perhaps constantly both 'in transit' and 'in storage' simultaneously." Councilman, 245 F. Supp. 2d at 321. This apt observation should have prompted a different legal conclusion.

All digital transmissions must be stored in RAM or on hard drives while they are being processed by computers during transmission. Every computer that forwards the packets that comprise an e-mail message must store those packets in memory while it reads their addresses, and every digital switch that makes up the telecommunications network through which the packets travel between computers must also store the packets while they are being

routed across the network. Since this type of storage is a fundamental part of the transmission process, attempting to separate all storage from transmission makes no sense.

Furthermore, in addition to storing the individual packets during routing, intermediate computers must temporarily store entire e-mail messages during transmission at various points along the route from sender to recipient. The technical specification for this type of e-mail transmission was adopted by the group that was coordinating standards for the Internet in 1982, see Jonathan B. Postel, RFC 821 - Simple Mail Transfer Protocol, available at http://www.faqs.org/rfcs/rfc821.html (last accessed May 19, 2004), and this standard for e-mail transmission was in use well before Congress adopted the ECPA in 1986. Therefore, when Congress acted, the fallacy of excluding from the scope of the Wiretap Act a message in storage at the time of interception was well-documented. The government's contemporaneous v. non-contemporaneous dichotomy accommodates this aspect of electronic technology; unlike Councilman's approach, it also makes sense in the real world.

The government's approach is also fully compatible with the portions of the ECPA that Councilman highlights in his argument. In a strange twist of logic, Councilman argues that Congress's broad definition of the term "electronic storage" supports his view that the e-mails at issue in this case were

protected by the Stored Communications Act and not by the Wiretap Act. Yet the legislative history demonstrates that Congress adopted this broad definition to enlarge privacy protections for personal data, not to exclude e-mails stored during transmission from the strong protections of the Wiretap Act.

Responding to concerns raised in the OTA report, Congress wanted to ensure that the messages and by-product files that are left behind after transmission and messages stored in a user's mailbox are protected from unauthorized access. The OTA identified four states during which a stored e-mail message could be accessed: 1) in the sender's terminal; 2) in the recipient's terminal; 3) in the recipient's paper files after the message was printed; and 4) in the service provider's electronic files when retained for administrative purposes. Electronic Surveillance, at 45. E-mails in the sender's and recipient's terminals could be accessed by "breaking into" those computers and retrieving the files. Id. at 48-49. As discussed in Section II, supra, the victim of such an attack had few legal remedies for such an invasion prior to the ECPA. The e-mails retained on the service provider's computers after transmission, which the report noted are primarily retained for "billing purposes and as a convenience in case the customer loses the message," could be accessed and possibly disclosed by the provider. Id. at 50. Prior to the ECPA, it was not clear whether the user had the right to challenge such a disclosure. Id.

Similar concerns applied to temporary financial records and personal data retained after transmission. Id. Given that background and evidence in the legislative history that Congress incorporated much of the OTA's report in the legislation, it appears that Congress had in mind these types of pre and post transmission "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," see 18 U.S.C. § 2510(17), when it established the definition of "electronic storage." There is no indication that it meant to exclude the type of storage used during transmission from the scope of the Wiretap Act.

It is also telling that virtually none of the discussions of electronic storage in House and Senate conference reports occur within the context of message transmission or the Wiretap Act. If, as the District Court and Councilman suggest, Congress intended to narrow the scope of the Wiretap Act by adopting a broad definition of "electronic storage," it would likely have discussed storage during transmission while it discussed the new provisions in the Wiretap Act.

In one of the few instances in which Congress discussed message storage within the context of the Wiretap Act, it explicitly distinguished messages in transit from messages in storage. In the section of the report discussing the

responsibilities of service providers to keep communications confidential, the House Committee stated:

> Section 2702(a) [the Stored Communications Act] generally prohibits the provider of a wire or electronic communication service to the public from knowingly divulging the contents of any communication while in electronic storage . . . . Similarly section 2511(3) of title 18 [the Wiretap Act], as amended, prohibits such a provider from divulging the contents of a communication while it is in transmission.

H.R. Rep. No. 99-647, at 65.

Likewise, there is nothing in the legislative record to indicate that Congress intended to reduce the protection for electronic communications by including the term "electronic storage" in its definition of "wire communication." Instead, as noted earlier, it appears that Congress included that provision in the ECPA simply to expand the protections for voicemails. The government's contemporaneous v. non-contemporaneous approach recognizes that Congress had to specifically include stored voicemails in the definition of "wire communication" to have the Wiretap Act apply to those communications. Without the explicit addition of voicemails to the scope of the Wiretap Act, these communications would have been regulated by the Stored Communications Act. Indeed, that is exactly what happened when Congress removed the explicit reference to "electronic storage" from the definition of "wire communication" in the Uniting and Strengthening America by Providing Appropriate Tools Required to

Intercept and Obstruct Terrorism (USA PATRIOT) Act, P.L. 107-56 § 209, 115 Stat. 283 (2001). See Konop, 302 F.3d at 878 ("By eliminating storage from the definition of wire communication, Congress essentially reinstated the pre-ECPA definition of 'intercept'--acquisition contemporaneous with transmission--with respect to wire communications."); Robert A. Pikowsky, An Overview of the Law of Electronic Surveillance Post September 11, 2001, 94 Law Libr. J. 601, 608 (2002) ("[T]he USA PATRIOT Act amended the statutory scheme and unambiguously brought voicemail under the Stored Communications Act.").

This result creates an analogy between electronic and wire communications: voicemails are to telephone calls in the wire communication context as messages stored in mailboxes are to e-mails in transit in the electronic communications context. See Pharmatrak, 329 F.3d at 18 ("ECPA amended the Federal Wiretap Act by extending to data and electronic transmissions the same protection already afforded to oral and wire communications."); Konop, 302 F.3d at 878 (Congress "accepted and implicitly approved the judicial definition of 'intercept' as acquisition contemporaneous with transmission."). The Government's approach to the ECPA is faithful to this analogy. Acquisitions of conversation stored in voicemailboxes, like messages stored in e-mailboxes, do not occur contemporaneously with communications; therefore, neither of these should be treated as intercepts under the Wiretap Act.

Telephone wiretaps and acquisitions of e-mails through the use of MUA recipe files, on the other hand, do occur contemporaneously with communications and should be considered intercepts under the Wiretap Act.

V. Existing Practices and Privacy Protections

The Government observes in its brief that its criminal investigators would stand to gain by the court's adoption of Councilman's interpretation: "If defendant's argument prevails, law enforcement would not violate the Wiretap Act by capturing the email without a wiretap order. Instead, law enforcement could rely on lesser legal process, with lesser judicial oversight, than is required under the Wiretap Act." As discussed in Section II, supra, the Stored Communications Act does not require the government to follow the procedures for obtaining a wiretap order. Officers can seize stored records for any crime for which they can get a search warrant; their search can extend to the limits of the Fourth Amendment; they do not need to report the progress of their search to courts; and defendants do not have an extra-constitutional right to suppress evidence from illegal searches.

The Justice Department's current policy guidance memorandum assumes that the type of communications at issue here fall under the purview of the Wiretap Act. See United States Department of Justice, Computer Crime and Intellectual Property Section, "Searching and Seizing Computers and Obtaining Electronic

Evidence in Criminal Investigations" § IV(d) (2002) ("Since its enactment in 1968 and amendment in 1986, [the Wiretap Act] has provided the statutory framework that governs real-time electronic surveillance of the contents of communications.") (emphasis added); Id. ("There is now a clear and uniform statutory distinction between stored electronic and wire communications, which are subject to [the Stored Communications Act], and contemporaneous interceptions of electronic and wire communications, which are subject to [the Wiretap Act]."). Therefore, it has been the Government's position that it had to obtain judicial authorization under the Wiretap Act to seize e-mails contemporaneously with their delivery. That practice would likely change under Councilman's interpretation of the Act. For example, the government states in its brief that "to implement wiretap orders on email accounts, the Federal Bureau of Investigation usually relies on the communication service providers to conduct the acquisitions." The providers use MUA recipe files similar to the one in this case to intercept, copy, and deliver the targeted e-mails to the government as they are being delivered. Under Councilman's narrow interpretation of the Act, the Government would no longer need to obtain a court-authorized wiretap order to conduct such surveillance. This would effectuate a dramatic change in Justice Department policy and mark a significant reduction in the public's right to privacy.

Such a change would not, however, be limited to the interception of e-mails. Under Councilman's approach, the government would be free to intercept all wire and electronic communications that are in temporary electronic storage without having to comply with the Wiretap Act's procedural protections. That means that the Government could install taps at telephone company switching stations to monitor phone conversations that are temporarily "stored" in electronic routers during transmission. See United States Telecom. Ass'n v. FCC, 227 F.3d 450, 464 (D.C. Cir. 2000) ("[In a digital telephone network,] a call is broken into a number of discrete digital data packets, each traveling independently through the network along different routes. Data packets are then reassembled in the proper sequence at the call's destination"); United States Congress, Office of Technology Assessment, Electronic Surveillance in a Digital Age 33 (1995) (stating that eighty percent of the telephone switches in the United States in 1991 were digital); see also 18 U.S.C. § 1002 (requiring telephone companies to ensure that the government retains the ability to intercept calls as the company installs new technologies). It could install "packet sniffer," software, computer programs that record the contents of all of the packets traveling through a network, on the servers of Internet Service Providers (ISPs) without having to comply with the Wiretap Act. See Kerr, supra, at 651 ("[A] system administrator (or a

twelve-year old computer hacker) can easily monitor all information flowing through a particular point in a network by writing a simple program.").

In short, Councilman's approach to the Wiretap Act would undo decades of practice and precedent regarding the scope of the Wiretap Act and would essentially render the Act irrelevant to the protection of wire and electronic privacy. Since I find it inconceivable that Congress could have intended such a result merely by omitting the term "electronic storage" from its definition of "electronic communication," I respectfully dissent.