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

Boudin, Chief Judge,
Torruella and Selya, Circuit Judges,
Cyr, Senior Circuit Judge,
Lynch, Lipez, and Howard, Circuit Judges.

John A. Drennan, Criminal Appellate Attorney, U.S. Department of Justice, with whom Michael J. Sullivan, U.S. Attorney, Paul G. Levenson, Assistant U.S. Attorney, and Paul K. Ohm, Trial Attorney, U.S. Department of Justice, were on brief, for appellant.

Andrew Good, with whom Matthew Zisow and Good & Cormier were on brief, for appellee.

Patricia L. Bellia and Peter P. Swire on brief for Senator Patrick J. Leahy, amicus curiae.

Marc Rotenberg and Marcia Hofmann on brief for Whitfield Diffie, Edward W. Felten, John R. Levine, Peter G. Neumann, and Bruce Schneier, amici curiae.

Shayana Kadidal and Carlos E. Gonzalez on brief, pro sese, amici curiae.

Orin S. Kerr on brief for Center for Democracy and Technology, Electronic Frontier Foundation, Electronic Privacy Information Center, American Library Association, American Civil Liberties Union, and Center for National Security Studies, amici curiae.

Opinion En Banc

August 11, 2005

LIPEZ, Circuit Judge. This case presents an important question of statutory construction. We must decide whether interception of an e-mail message in temporary, transient electronic storage states an offense under the Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522. The government believes it does, and indicted Councilman under that theory. The district court disagreed and dismissed the indictment. A divided panel of this court affirmed. We granted review en banc and now reverse.[1]

I.

A. An Introduction to Internet E-mail

The Internet is a network of interconnected computers. Data transmitted across the Internet are broken down into small "packets" that are forwarded from one computer to another until they reach their destination, where they are reconstituted. 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, the World Wide Web, or instant messaging -- has its own protocol for using packets of data to transmit information from one place to another. The e-mail protocol is known as Simple Mail Transfer Protocol ("SMTP").

[1]We acknowledge with gratitude the assistance of amici curiae.

After a user composes a message in an e-mail client program,[2] a program called a mail transfer agent ("MTA") formats that message and sends it to another program that "packetizes" it and sends the 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 addresses of their final destinations, and then determines where to send them next. 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 (Apr. 2001), at http://www.ietf.org/rfc/rfc2821.txt; Jonathan B. Postel, RFC 821: Simple Mail Transfer Protocol (Aug. 1982), at http://www.ietf.org/rfc/rfc821.txt ("RFC 821"). Sometimes messages cannot be transferred immediately and must be saved for later delivery. Even when delivery is immediate, intermediate computers often retain backup copies, which they delete later. This 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 delivery agent ("MDA") accepts the message from the MTA, determines which user should receive the message, and performs the actual delivery by placing the message in that user's mailbox. One popular MDA is

[2]Sometimes called a mail user agent ("MUA").

"procmail," which is controlled by short programs or scripts called "recipe files." These recipe files can be used in various ways. For example, a procmail recipe can instruct the MDA to deposit mail addressed to one address into another user's mailbox (e.g., 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 MDA has deposited a message into the recipient's mailbox, the recipient simply needs to use an e-mail client program to retrieve and read the message.[3] While the journey from sender to recipient may seem rather involved, it usually takes just a few seconds, with each intermediate step taking well under a second. See, e.g., W. Houser et al., RFC 1865: EDI Meets the Internet (Jan. 1996), at http://www.ietf.org/rfc/rfc1865.txt ("For a modest amount of data with a dedicated connection, a message transmission would occur in a matter of seconds . . . .").

B. Facts Alleged in the Indictment

Defendant-appellee Bradford C. Councilman was Vice President of Interloc, Inc., which ran an online rare and out-of-print book listing service. As part of its service, Interloc gave book dealer customers an e-mail address at the domain "interloc.com" and acted as the e-mail provider. Councilman managed the e-mail service and the dealer subscription list.

[3]In some cases, the e-mail client program is accessed through the World Wide Web. This does not change the present discussion.

According to the indictment, in January 1998, Councilman directed Interloc employees to intercept and copy all incoming communications to subscriber dealers from Amazon.com, an Internet retailer that sells books and other products. Interloc's systems administrator modified the server's procmail recipe so that, before delivering any message from Amazon.com to the recipient's mailbox, procmail would copy the message and place the copy in a separate mailbox that Councilman could access. Thus, procmail would intercept and copy all incoming messages from Amazon.com before they were delivered to the recipient's mailbox, and therefore, before the intended recipient could read the message. This diversion intercepted thousands of messages, and Councilman and other Interloc employees routinely read the e-mail messages sent to Interloc subscribers in the hope of gaining a commercial advantage.

C. Procedural History

On July 11, 2001, a grand jury returned a two-count indictment against Councilman. Count One charged him under 18 U.S.C. § 371, the general federal criminal conspiracy statute, for conspiracy to violate the Wiretap Act, 18 U.S.C. § 2511,[4] by intercepting electronic communications, disclosing their contents, using their contents, and causing a person providing an electronic

[4]The Wiretap Act was amended in relevant respects in 2001, after Councilman's alleged conduct and, for that matter, after the indictment. Accordingly, all statutes are cited according to the United States Code as of 1998 except where specified otherwise.

communications service to divulge the communications' contents to persons other than the addressees.[5] The object of the conspiracy was to exploit the content of e-mail from Amazon.com to dealers in order to develop a list of books, learn about competitors, and attain a commercial advantage for Interloc and its parent company.[6]

The parties stipulated to certain undisputed facts: the procmail recipe worked only within the confines of Interloc's computer; at all times at which 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 system"; and each e-mail message, while traveling through wires, was an "electronic communication" under 18 U.S.C. § 2510(12).

Councilman moved to dismiss the indictment for failure to state an offense under the Wiretap Act, arguing that the intercepted e-mail messages were in "electronic storage," as defined in 18 U.S.C. § 2510(17), and therefore were not, as a

---

[5]The indictment contained several errors. It alleged conspiracy to disclose the contents of unlawfully intercepted electronic communications under 18 U.S.C. § 2511(1)(a), which should have read § 2511(1)(c), and conspiracy to use the contents of unlawfully intercepted electronic communications under § 2511(1)(c), which should have read § 2511(1)(d) or § 2511(1)(b). No superseding indictment corrected these errors. Councilman has not raised this issue, and we assume, for purposes of this appeal only, that the indictment charged the conspiracy correctly.

[6]Count Two, which alleged conspiracy to violate the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B), was voluntarily dismissed by the government.

matter of law, subject to the prohibition on "intercept[ing] . . . electronic communication[s]," 18 U.S.C. § 2511(1)(a). The district court initially denied the motion to dismiss. As trial preparation began, however, the district court sua sponte reconsidered its decision in light of the then-recently decided case of Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002). After further briefing, the district court granted Councilman's motion to dismiss Count One, ruling that the messages were not, at the moment of interception, "electronic communications" under the Wiretap Act. United States v. Councilman, 245 F. Supp. 2d 319 (D. Mass. 2003).

A divided panel of this court affirmed. United States v. Councilman, 373 F.3d 197 (1st Cir. 2004). The majority concluded that, because the definition of "wire communication" includes "electronic storage" but the definition of "electronic communication" does not, the Wiretap Act's prohibition on "intercept[ion]" does not apply to messages that are, even briefly, in "electronic storage." Id. at 200-04. The full court granted the government's petition for rehearing en banc. 385 F.3d 793 (1st Cir. 2004) (per curiam). Because this is an appeal of an order dismissing an indictment on "purely legal" grounds, our review is de novo, United States v. Lopez-Lopez, 282 F.3d 1, 9 (1st Cir. 2002), and we assume the truth of the facts alleged in the indictment, see Bank of Nova Scotia v. United States, 487 U.S. 250, 261 (1988).

II.

The Wiretap Act of 1968[7] specified, inter alia, the conditions under which law enforcement officers could intercept wire communications, and the penalties for unauthorized private interceptions of wire communications. As amended by the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 ("ECPA"), the Act makes it an offense to "intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1). Two terms are at issue here: "electronic communication" and "intercept."

Councilman contends that the e-mail messages he obtained were not, when procmail copied them, "electronic communication[s]," and moreover the method by which they were copied was not "intercept[ion]" under the Act. Because these contentions raise important questions of statutory construction with broad ramifications, we discuss in some detail the Act's text, structure, and legislative history. We conclude that Councilman's interpretation of the Wiretap Act is inconsistent with Congress's intent. We then turn to whether Councilman had fair warning that the Act would be construed to cover his alleged conduct in a criminal case, and whether the rule of lenity or other principles

[7]Formally known as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, §§ 801-804, 82 Stat. 211 (codified as amended at 18 U.S.C. §§ 2510-2522).

require us to construe the Act in his favor. We find no basis to apply any of the fair warning doctrines.

A. "Electronic Communication"

The government contends that "electronic communication" means what it says, and no less: "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," with four specific exceptions not relevant here. 18 U.S.C. § 2510(12). Councilman argues, however, that Congress intended to exclude any communication that is in (even momentary) electronic storage. In his view, "electronic communication[s]" under the Wiretap Act are limited to communications traveling through wires between computers.[8] Once a message enters a computer, he says, the message ceases (at least temporarily) to be an electronic communication protected by the Wiretap Act. He claims that Congress considered communications in computers to be worthy of less protection than communications in wires because users have a lower expectation of privacy for electronic communications that are in electronic storage even fleetingly, and that the Act embodies this understanding.

[8]We understand Councilman to refer to communications in "wires" in order to exclude communications within computers, rather than to exclude wireless connections.

1. Text

We begin, as we must, with the statute's text. United States v. Rosa-Ortiz, 348 F.3d 33, 36 (1st Cir. 2003). As noted above, the statutory definition of "electronic communication" is broad and, taken alone, would appear to cover incoming e-mail messages while the messages are being processed by the MTA.

Councilman argues, however, that the plain text of the statute exempts electronic communications that are in storage from the purview of the Wiretap Act. He contends that the definition of "electronic communication" must be read alongside the definition of "wire communication" and limited by what the latter includes but the former does not. The ECPA amended the 1968 definition of "wire communication" to specify that "such term includes any electronic storage of such communication." 18 U.S.C. § 2510(1); ECPA § 101(a)(1)(D), 100 Stat. at 1848. By contrast, the definition of "electronic communication" does not mention electronic storage. See 18 U.S.C. § 2510(12).[9] Therefore, Councilman infers, Congress

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

> [A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects . . . commerce, but . . . not includ[ing] --
> (A) any wire or oral communication;
> (B) any communication made through a tone-only paging device;
> (C) any communication from a tracking device . . . or
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

intended wire communications, but not electronic communications, to include electronic storage. Moreover, Congress defined "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 Councilman, 245 F. Supp. 2d at 320 (describing this definition as "extraordinarily -- indeed, almost breathtakingly -- broad"). Since the parties stipulated that the messages in this case were "in the random access memory (RAM) or in the hard disks, or both, within Interloc's computer system" at the time of the interception, those messages fall under the statutory definition of "storage."

As often happens under close scrutiny, the plain text is not so plain. The statute contains no explicit indication that Congress intended to exclude communications in transient 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 an inferential leap. He infers that Congress intended to exclude communications in transient storage from the definition of "electronic communication," regardless of whether they are in the 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.

Councilman's basis for making this leap is a canon of construction: "[W]here 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." Russello v. United States, 464 U.S. 16, 23 (1983) (quotation marks and citation omitted; alteration in original); see also Trenkler v. United States, 268 F.3d 16, 23 (1st Cir. 2001) (characterizing the maxim as a canon of construction). Reliance on a canon of construction to support the inference belies the availability of a plain text argument. Rather, it confirms that the text of the statute is ambiguous with regard to the communications at issue.

The question, then, is whether Councilman's inferential leap, based on a canon of construction, is justified. The Russello maxim -- which is simply a particular application of the classic principle expressio unius est exclusio alterius -- assumes that Congress acts carefully and deliberately in including terms in one part of a statute and omitting them in another. See Barnhart v. Peabody Coal Co., 537 U.S. 149, 168 (2003) ("We do not read the enumeration of one case to exclude another unless it is fair to suppose that Congress considered the unnamed possibility and meant to say no to it.").

Sometimes that is a reasonable assumption; sometimes it is not. "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." Springer v. Gov't of Phil. Islands, 277 U.S. 189, 206 (1928); United States v. Vonn, 535 U.S. 55, 65 (2002) ("[T]he canon . . . is only a guide, whose fallibility can be shown by contrary indications that adopting a particular rule or statute was probably not meant to signal any exclusion of its common relatives.").

The maxim upon which Councilman relies is most apt when Congress enacts a new, self-contained statute, and two provisions of that act, drafted with parallel language, differ in that one provision uses a term, but the other provision, where it would be equally sensible to use that term if Congress desired it to apply, conspicuously omits it. Under such conditions, the maxim's interpretive value is at its apex because the underlying inference of legislative intent is most plausible. See Field v. Mans, 516 U.S. 59, 75-76 (1995) ("The more apparently deliberate the contrast, the stronger the inference, as applied, for example, to contrasting statutory sections originally enacted simultaneously in relevant respects.")

If the statute's language, structure, or circumstances of enactment differ from that idealized picture, the canon's force is diminished. For example, if the language of the two provisions at

issue is not parallel, then Congress may not have envisioned that the two provisions would be closely compared in search of terms present in one and absent from the other. "The Russello presumption -- that the presence of a phrase in one provision and its absence in another reveals Congress'[s] design -- grows weaker with each difference in the formulation of the provisions under inspection." City of Columbus v. Ours Garage & Wrecker Serv., Inc., 536 U.S. 424, 435-36 (2002); see also Clay v. United States, 537 U.S. 522, 529 (2003) (rejecting Russello-based argument because two statutory provisions were not parallel). Similarly, where the history of the two provisions is complex, the canon may be a less reliable guide to Congressional intent. For example, if the first provision was already part of the law, whereas the second is entirely new, Congress may have paid less attention to subtle differences between the two. Cf. Moreno Rios v. United States, 256 F.2d 68, 71 (1st Cir. 1958) (Magruder, C.J.) (the expressio unius inference "is pretty weak when applied to acts of Congress enacted at widely separated times").

In attempting to determine whether Congress intended the term "electronic communication" to exclude communications in momentary storage, the expressio unius maxim is not particularly helpful. Put differently, though it may be "presumed that Congress acts intentionally and purposely in the disparate inclusion or

exclusion," Russello, 464 U.S. at 23, that presumption may be rebutted. That is the case here.

First, the definitions of "wire communication" and "electronic communication" in the Wiretap Act are not parallel. The former is defined in a single lengthy clause that specifies multiple independent criteria, with the electronic storage clause tacked onto the end. See 18 U.S.C. § 2510(1). The revised definition hews closely to its original definition in the 1968 Wiretap Act; the ECPA simply amended that definition by replacing the phrase "communication" with "aural transfer," making certain modifications not relevant here, and, of course, adding the clause "and such term includes any electronic storage of such communication."[10] See ECPA § 101(a)(1)(D), 100 Stat. at 1848. By

---

[10]Before the ECPA, the definition of "wire communication" read:

> "Wire 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.

18 U.S.C. § 2510(12) (1972). As amended by the ECPA in 1986, that definition read:

> "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 switching station) furnished or operated by any person engaged in providing or operating such

contrast, "electronic communication" is first defined in broad terms which are narrowed by four specific exclusions enumerated in separate subparagraphs. See 18 U.S.C. § 2510(12). The definition was drafted from scratch as part of the ECPA. ECPA § 101(a)(6), 100 Stat. at 1848-49.

Second, any expressio unius inference that can be drawn from the presence of the electronic storage clause in one definition and its absence from another is in tension with a much more compelling -- and directly contrary -- expressio unius inference drawn from the same statutory provisions: Congress knew how to, and in fact did, explicitly exclude four specific categories of communications from the broad definition of "electronic communication." See ECPA § 101(a)(6)(C).[11] Yet

---

> 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, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit.

18 U.S.C. § 2510(12) (1988).

[11]In 1994, Congress deleted the exclusion of cordless phone conversations, see Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, tit. II, § 202(a)(1), 108 Stat. 4279, 4291 (1994), and two years later, added an exclusion for electronic funds transfer information, see Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, tit. VII, § 731(1)(C), 110 Stat. 1214, 1303 (1996). Thus, by the time of the conduct alleged in the indictment, Congress had enacted five separate exclusions from the definition of "electronic communication," and deleted one of them, on three separate occasions.

Congress never added the exclusion urged by Councilman: "any electronic communication in electronic storage." This interpretative principle then applies: "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." TRW v. Andrews, 534 U.S. 19, 28 (2001) (quotation marks and citation omitted).

In short, the ECPA's plain text does not clearly state whether a communication is still an "electronic communication" within the scope of the Wiretap Act when it is in electronic storage during transmission. Applying canons of construction does not resolve the question. Given this continuing ambiguity, we turn to the legislative history.

2. Legislative History

As we explain below, the purpose of the broad definition of electronic storage was to enlarge privacy protections for stored data under the Wiretap Act, not to exclude e-mail messages stored during transmission from those strong protections. Moreover, Congress's sole purpose in adding electronic storage to the definition of "wire communication" was to protect voice mail, and not to affect e-mail at all.

a. Background of the ECPA

By the early 1980s, the advent of electronic communications, principally e-mail, suggested to many that the

Wiretap Act needed revision. To update the Act, Senator Patrick Leahy introduced the Electronic Communications Privacy Act of 1985. See S. 1667, 99th Cong. (1985), reprinted in 131 Cong. Rec. S11,795 (Sept. 19, 1985). That bill would have amended the Act by striking out the existing definition of "wire communication," substituting the phrase "electronic communication" for "wire communication" throughout the Act, and subsuming wire communications within the newly-defined term "electronic communication." See id. § 101.

Shortly after the bill was introduced, the Congressional Office of Technology Assessment released a long-awaited study of the privacy implications of electronic surveillance. See Office of Technology Assessment, Federal Government Information Technology: Electronic Surveillance and Civil Liberties, available at http://www.wws.princeton.edu/~ota/disk2/1985/8509_n.html (Oct. 1985) ("OTA Report"). The report identified the different points at which an e-mail message could be intercepted:

> There are at least five discrete stages at which an electronic mail message could be intercepted and its contents divulged to an unintended receiver: at the terminal or in the electronic files of the sender, while being communicated, in the electronic mailbox of the receiver, when printed into hardcopy, and when retained in the files of the electronic mail company for administrative purposes. Existing law offers little protection.

Id. at 48. It emphasized that "interception of electronic mail at any stage involves a high level of intrusiveness and a significant threat to civil liberties." Id. at 50 (emphasis added).

The Department of Justice ("DOJ") was the principal opponent of the original bill. DOJ conceded that "the level of intrusion during [an e-mail message's] transmission is higher than when it is stored," but urged that "the interception of electronic mail should include some but not all of the procedural requirements of [the Wiretap Act]." Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice, House Comm. on the Judiciary, 99th Cong. 214, 230 (1986) ("House Hearings") (statement of James Knapp, Deputy Assistant Attorney General, Criminal Division, U.S. Dep't of Justice). DOJ asked Congress to treat prospective surveillance of electronic communications differently from surveillance of wire communications in three specific respects that are related solely to law enforcement and are not relevant here. See id. at 215, 232-33. DOJ's willingness to extend some of the Wiretap Act's protections to e-mail did not, however, extend to "the time after a specific communication has been sent and while it is in the electronic mail firm's computers but has not been delivered, or has been delivered to the electronic mailbox but has not been received by the recipient." Id. at 234. In such cases, DOJ suggested, the message should be treated like first-class mail, and law enforcement should be able to seize it with an ordinary search warrant. Id.

A new version of the bill was introduced to meet some, but not all, of DOJ's concerns. See Electronic Communications Privacy Act of 1986, S. 2575, 99th Cong. (1986). The new bill rejected DOJ's preferred solution and instead added electronic communications to the Wiretap Act's existing prohibitions on interception of wire communications. As the House report made clear, Congress intended to give the term "electronic communication" a broad definition:

> The term 'electronic communication' is intended to cover a broad range of communication activities . . . . 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). Communications consisting solely of data, for example . . . would be electronic communications.

H.R. Rep. No. 99-647 (1986), at 35. By incorporating electronic communications into the Wiretap Act, the bill largely rejected DOJ's view that e-mail should receive no (or little) more protection than first class mail. See H.R. Rep. No. 99-647, at 22 (explaining why e-mail differs from regular mail). Nevertheless, because some of DOJ's specific concerns were addressed, DOJ acknowledged that "the bill has been substantially modified to

accommodate our concerns" and supported it. Id. at 30-31.

b. The broad definition of electronic storage

Responding to concerns raised in the OTA Report, Congress sought to ensure that the messages and by-product files that are left behind after transmission, as well as messages stored in a user's mailbox, are protected from unauthorized access. E-mail messages in the sender's and recipient's computers could be accessed by electronically "breaking into" those computers and retrieving the files. OTA Report at 48-49. Before the ECPA, the victim of such an attack had few legal remedies for such an invasion. Furthermore, the e-mail messages 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. Before 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 this background and the evidence in the legislative history that Congress responded to the OTA Report in refining the legislation, see, e.g., House Hearings at 42-73, 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." Its aim was simply to protect such data. See infra Part II.C.1 (describing the Stored Communications Act). There is no indication that it meant to exclude the type of storage used during transmission from the scope of the Wiretap Act.

c. The electronic storage clause in the definition of "wire communication"

The original version of the ECPA of 1986 included the definition of "electronic storage" as it reads today, but did not include electronic storage in the definition of "wire communication." 132 Cong. Rec. S7,991 (June 19, 1986). Neither Senator Leahy's floor statement upon introducing the bill nor the staff bill summary mentioned voice mail in the context of the Wiretap Act amendments. See id.; cf. H.R. Rep. No. 99-647, at 63 (mentioning voice mail in the context of Stored Communications Act). Voice mail had not, apparently, been a major subject of discussion in the context of the ECPA.[12]

Similarly, when Representative Kastenmeier introduced his identical bill in the House, he did not mention voice mail in his remarks. See 132 Cong. Rec. H4,039 (June 23, 1986). The electronic storage clause in the wire communications definition first appeared in Senate committee markup after the House had already passed the bill without the clause. See 132 Cong. Rec.

[12]For example, it was not mentioned in the OTA Report or DOJ's comments in the House or Senate hearings.

S14,441 (Oct. 1, 1986). Senator Leahy, in his statement in support of the amended bill, specifically mentioned voice mail, which he had not done in his remarks earlier that year, and the staff summary explained that one effect of the amended bill was that "[w]ire communications in storage, like voice mail, remain wire communications." Id. (emphasis added).[13]

If the addition of the electronic storage clause to the definition of "wire communication" was intended to remove electronic communications from the scope of the Wiretap Act for the brief instants during which they are in temporary storage en route to their destinations -- which, as it turns out, are often the points where it is technologically easiest to intercept those communications -- neither of the Senate co-sponsors saw fit to mention this to their colleagues, and no one, evidently, remarked upon it. No document or legislator ever suggested that the addition of the electronic storage clause to the definition of "wire communication" would take messages in electronic storage out of the definition of "electronic communication." Indeed, we doubt that Congress contemplated the existential oddity that Councilman's interpretation creates: messages -- conceded by stipulation to be

[13]The summary also noted that "[c]ertain electronic communications are exempted from the coverage of the bill" and listed the exceptions contained in 18 U.S.C. § 2511(2)(g), none of which are relevant here. Id. Nowhere did it suggest that electronic communications that were briefly in temporary storage were exempted from the coverage of the bill.

electronic communications -- briefly cease to be electronic communications for very short intervals, and then suddenly become electronic communications again. Cf. H.R. Rep. No. 99-647, at 35 ("The term 'electronic communication' is intended to cover a broad range of communication activities . . . . Communications consisting solely of data . . . would be electronic communications.").

In sum, the legislative history indicates that Congress included the electronic storage clause in the definition of "wire communication" provision for the sole reason that, without it, access to voicemail would have been regulated solely by the Stored Communications Act. Indeed, that is exactly what happened when Congress later 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, Pub. L. No. 107-56, tit. II, § 209(1)(A), 115 Stat. 272, 283 (2001). See 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.").

3. Conclusion

We conclude that the term "electronic communication" includes transient electronic storage that is intrinsic to the communication process for such communications. That conclusion is consistent with our precedent. See Blumofe v. Pharmatrak, Inc. (In re Pharmatrak Privacy Litig.), 329 F.3d 9, 21 (1st Cir. 2003) (a rigid "storage-transit dichotomy . . . may be less than apt to address current problems");[14] see also Hall v. EarthLink Network, Inc., 396 F.3d 500, 503 n.1 (2d Cir. 2005) (rejecting arguments that "communication over the Internet can only be electronic communication while it is in transit, not while it is in electronic storage"). Consequently, in this context we reject Councilman's proposed distinction between "in transit" and "in storage."

B. "Intercept"

Even though we conclude that the temporarily stored e-mail messages at issue here constitute electronic communications within the scope of the Wiretap Act, the statute also requires the conduct alleged in the indictment to be an "intercept[ion]." 18 U.S.C. § 2511(1) (making it an offense to "intentionally intercept[], endeavor[] to intercept, or procure[] any other person

[14] Pharmatrak arose from a tracking program that surreptitiously transmitted information about users' web browsing activity to a third party. Web sites using the service added to their web pages an instruction to download an invisible image from the Pharmatrak web site. This caused the user's computer to communicate directly to Pharmatrak's web server, which recorded information about the user and her browsing activity. See id. at 13-14.

to intercept or endeavor to intercept, any . . . electronic communication"). The term "intercept" is defined broadly 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." Id. § 2510(4).

Councilman's core argument on appeal is that because the messages at issue, when acquired, were in transient electronic storage, they were not "electronic communication[s]" and, therefore, section 2511(1)'s prohibition on "intercept[ion]" of any "electronic communication" did not apply. That is the argument that we have now rejected in holding that an e-mail message does not cease to be an "electronic communication" during the momentary intervals, intrinsic to the communication process, at which the message resides in transient electronic storage. See supra Part II.A.

Councilman's appeal does not provide any other basis for finding that the acquisitions were not "intercept[ions]" of "electronic communication[s]." To be sure, Councilman does argue that "Congress intended 'intercept' to cover acquisitions 'contemporaneous with transmission.'" However, his entire argument on this point is based on the theory, as he writes in his brief, that "[c]ourts uniformly have understood 'electronic storage' to negate the 'contemporaneous with transmission' element of a Wiretap Act 'intercept,'" and therefore "an e-mail in 'electronic storage'

. . . cannot by definition be acquired 'contemporaneous with transmission.'" That argument is simply a variation on, and entirely subsumed within, his primary argument concerning "storage" -- the very argument that we have now rejected.

Consequently, this appeal does not implicate the question of whether the term "intercept" applies only to acquisitions that occur contemporaneously with the transmission of a message from sender to recipient or, instead, extends to an event that occurs after a message has crossed the finish line of transmission (whatever that point may be). See Pharmatrak, 329 F.3d at 21-22 (noting that the concept of a contemporaneity or real-time requirement, which evolved in other factual contexts, may not be apt to address issues involving the application of the Wiretap Act to electronic communications). We therefore need not decide that question. See United States v. Moran, 393 F.3d 1, 12 (1st Cir. 2004) (noting that, in certain circumstances, an appellee is obliged, on pain of waiver, to raise additional or alternative bases for affirming a favorable judgment); Raxton Corp. v. Anania Assocs., Inc., 668 F.2d 622, 624 (1st Cir. 1982) (emphasizing the importance of "[t]he presentation on appeal of all viable justifications of a judgment").

That ends this aspect of the matter. Because the facts of this case and the arguments before us do not invite consideration of either the existence or the applicability of a

contemporaneity or real-time requirement, we need not and do not plunge into that morass. We note, however, that even were we prepared to recognize a contemporaneity or real-time requirement -- a step that we do not take today -- we think it highly unlikely that Councilman could generate a winning argument in the circumstances of this case. Any such argument would entail a showing that each transmission was complete at the time of acquisition and, therefore, that the definition of "intercept" does not cover the acquisitions. Such a showing would appear to be impossible since we have concluded that the messages were electronic communications, and it is undisputed that they were acquired while they were still en route to the intended recipients.

C. Intersection of the Wiretap Act and the Stored Communications Act

Thus far we have considered only the Wiretap Act, not the Stored Communications Act, 18 U.S.C. §§ 2701-2712, because the indictment only alleged a violation of the former. Councilman argues that acquisition of electronic communications in temporary electronic storage is regulated by the Stored Communications Act. From this he infers that such acquisition is not regulated by the Wiretap Act, or that, at minimum, the potential overlap implicates the rule of lenity or other doctrines of "fair warning." Consequently, we must delve into the "complex, often convoluted" intersection of the Wiretap Act and Stored Communications Act. United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).

1. The Stored Communications Act's Coverage

While drafting the ECPA's amendments to the Wiretap Act, Congress also recognized that, with the rise of remote computing operations and large databanks of stored electronic communications, threats to individual privacy extended well beyond the bounds of the Wiretap Act's prohibition against the "interception" of communications. These types of stored communications -- including stored e-mail messages -- were not protected by the Wiretap Act. 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." S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557.

Congress added Title II to the ECPA to halt these potential intrusions on individual privacy. This title, commonly referred to as the Stored Communications Act,[15] established new punishments for accessing, without (or in excess of) authorization, an electronic communications service facility and thereby obtaining access to a wire or electronic communication in electronic storage. 18 U.S.C. § 2701(a). Another provision bars electronic communications service providers from "divulg[ing] to any person or

[15]As noted, Title I of the ECPA amended the 1968 Wiretap Act. By "Wiretap Act," we mean the 1968 Wiretap Act as amended by Title I of the ECPA. We refer to Title II of the ECPA simply as the Stored Communications Act.

entity the contents of a communication while in electronic storage by that service." Id. § 2702(a)(1).

The privacy protections established by the Stored Communications Act were intended to apply to two categories of communications defined by the statutory term "electronic storage":

> (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.

18 U.S.C. § 2510(17); id. § 2711(a) (incorporating Wiretap Act definitions into Stored Communications Act). The first category, which is relevant here, refers to temporary storage, such as when a message sits in an e-mail user's mailbox after transmission but before the user has retrieved the message from the mail server.

Councilman's conduct may appear to fall under the Stored Communications Act's main criminal provision:

> (a) Offense. Except as provided in subsection (c) of this section 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 . . . .

18 U.S.C. § 2701(a). At the same time, Councilman would arguably be exempted by the Stored Communications Act's provider exception: "Subsection (a) of this section does not apply with respect to conduct authorized (1) by the person or entity providing a wire or electronic communications service." Id. § 2701(c). Under this theory, § 2701(c)(1) establishes virtually complete immunity for a service provider that "obtains, alters, or prevents authorized access to" e-mail that is "in electronic storage" in its system. See Fraser, 352 F.3d at 115 ("[W]e read § 2701(c) literally to except from Title II's protection all searches by communications service providers."). The district court surmised that § 2701(a) would have covered Councilman's conduct but that § 2701(c)(1) exempted him. Councilman, 245 F. Supp. 2d at 320.

A second provision of the Stored Communications Act prohibits "a person or entity providing an electronic communication service to the public [from] knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). Yet this provision, too, has service provider exceptions, permitting a provider to divulge an electronic communication "to a person employed or authorized or whose facilities are used to forward such communication to its destination," id. § 2702(b)(4), or "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that

service," id. § 2702(b)(5). We assume, dubitante, that one or both of these provisions would exempt Councilman under § 2702.

On this premise, he argues that if he is not liable under the Stored Communications Act, then he cannot be liable under the Wiretap Act either. Since Congress enacted the ECPA as a package, he says, it did not intend to lay traps in the overlap between the two titles. If conduct that potentially falls under both titles is exempt from one of them, then that exemption provides a "safe harbor" and the conduct does not violate the other title either.

We find this argument unpersuasive. In general, if two statutes cover the same conduct, the government may charge a violation of either. See United States v. Herring, 993 F.2d 784, 788 n.4 (11th Cir. 1993) (en banc) ("The overlapping coverage of the Wiretap Act and the Communications Act [of 1934] presents no problem. In such a case, the prosecution has the right to select the statute under which the indictment will be brought."). Moreover, the exceptions in the Stored Communications Act do not, by their terms, apply to the Wiretap Act. The exception in § 2701(c) specifically limits its application by stating that "[s]ubsection (a) of this section does not apply . . . to conduct authorized" by the service provider. (Emphasis added). The § 2701(c)(1) provider exception's breadth presents a striking contrast to the Wiretap Act's own, much narrower provider exception:

> It shall not be unlawful under this chapter for . . . an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service . . . .

Id. § 2511(2)(a)(i) (emphasis added). It is indisputable that the Wiretap Act's narrower service provider exception would not protect Councilman. His alleged conduct was clearly not "a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." If there were any doubt remaining, it would be resolved by the Wiretap Act's express provision that the only exceptions to its prohibitions are those specifically listed within the Wiretap Act, not those found in other laws. See 18 U.S.C. § 2511(1) (prohibitions apply "[e]xcept as otherwise specifically provided in this chapter [the Wiretap Act, 18 U.S.C. §§ 2510-2522]") (emphasis added).

2. Fair Warning

Councilman argues in the alternative that the two titles are sufficiently confusing that principles of fair warning require dismissal of the indictment. Those principles are expressed in the law through three related doctrines: the rule of lenity, the vagueness doctrine, and the prohibition against unforeseeably expansive judicial constructions. See United States v. Lanier, 520

U.S. 259, 266-67 (1997); United States v. Hussein, 351 F.3d 9, 14-16 (1st Cir. 2003). We address each in turn.

a. Lenity

Under the rule of lenity, grievous ambiguity in a penal statute is resolved in the defendant's favor. See Lanier, 520 U.S. at 266. "The simple existence of some statutory ambiguity, however, is not sufficient to warrant application of that rule, for most statutes are ambiguous to some degree." Muscarello v. United States, 524 U.S. 125, 138-39 (1998). Rather, the rule only applies if "there is a grievous ambiguity or uncertainty in the statute." Id. at 139 (quotation marks and citation omitted) (emphasis added). Furthermore, lenity "applies only if, after seizing everything from which aid can be derived, [a court] can make no more than a guess as to what Congress intended." Reno v. Koray, 515 U.S. 50, 65 (1995) (quotation marks and citation omitted); accord United States v. Balint, 201 F.3d 928, 935 (7th Cir. 2000) ("The rule of lenity is unavailable to us if the purported ambiguity in a statute can be resolved through normal methods of statutory construction.").

Here, while the statute contains some textual ambiguity, it is not "grievous." We have construed it using traditional tools of construction, particularly legislative history, and lenity is therefore inapplicable. See, e.g., Dixson v. United States, 465 U.S. 482, 491 (1984) ("If the legislative history fails to clarify the statutory language, our rule of lenity would compel us to

construe the statute in favor of petitioners, as criminal defendants in these cases.") (emphasis added).

Furthermore, Congress specifically anticipated that communication service providers might, in good faith, misapprehend their lawful ability to intercept or disclose communications in certain circumstances. Congress addressed that problem with a broad, affirmative good faith defense:

> A good faith reliance on . . . (3) a good faith determination that [§ 2511(3)] permitted the conduct complained of[] is a complete defense against any civil or criminal action brought under [the Wiretap Act] or any other law.

18 U.S.C. § 2520(d)(3).[16] Section 2511(3), in turn, authorizes a communication service provider to divulge a communication to one other than the recipient in four specified circumstances.[17] Thus,

---

[16]Section 2520(d) originated with the 1968 Wiretap Act, which specified that "[a] good faith reliance on a court order or on the provisions of [18 U.S.C. § 2518(7) (emergency wiretaps)] shall constitute a complete defense to any civil or criminal action brought under this chapter." Pub. L. No. 90-851, sec. 802, § 2520, 82 Stat. at 223. After various other amendments not relevant here, see generally Jacobson v. Rose, 592 F.2d 515, 522-23 & nn. 13-15 (9th Cir. 1978) (recounting pre-ECPA history of provision), the ECPA broadened the types of authority on which the defense could be based. ECPA § 103, 100 Stat. at 1854.

[17]Those circumstances are:

> (i) as otherwise authorized in section 2511(2)(a) or 2517 . . .
> (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;
> (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

Congress contemplated that service providers might, in good faith, misunderstand the limits of their authority on a particular set of facts, and provided a statutory mechanism to solve this problem. We may neither expand the good faith defense's scope, nor convert it from a fact-based affirmative defense to a basis for dismissing an indictment on legal grounds.[18]

b. Vagueness

The vagueness doctrine bars enforcement of a statute whose terms are "so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application." Lanier, 520 U.S. at 266 (quotation marks and citation omitted). But vagueness is more than just "garden-variety, textual ambiguity." Sabetti v. Dipaolo, 16 F.3d 16, 18 (1st Cir. 1994) (Breyer, C.J.). "Many statutes will have some inherent vagueness, for '[i]n most English words and phrases there lurk uncertainties.'" Rose v. Locke, 423 U.S. 48, 49-50 (1975) (per curiam) (citation omitted). But a statute is unconstitutionally vague only if it "prohibits . . . an act in terms so uncertain that

---

> (iv) [if the communications] were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.
>
> 18 U.S.C. §§ 2511(3)(b)(i)-(iv).

[18]Nothing in this opinion prejudices Councilman's ability to argue the good faith defense in subsequent proceedings.

persons of average intelligence would have no choice but to guess at its meaning and modes of application." Hussein, 351 F.3d at 14.

The Wiretap Act is not unconstitutionally vague in its application here. From its text, a person of average intelligence would, at the very least, be on notice that "[e]xcept as otherwise specifically provided in" the Act, "electronic communication[s]," which are defined expansively, may not be "intercepted." 18 U.S.C. § 2511(1)(a). An exception is provided for electronic communication service providers, but it only applies to "activity which is a necessary incident to the rendition of [the] service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2511(2)(a)(i). The Act puts the service provider on notice of both the prohibited conduct and the narrow provider exception. That is adequate notice.

c. Unforeseeably expansive interpretation

Finally, the third branch of fair warning doctrine "bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope." Lanier, 520 U.S. at 266. This doctrine principally "bars 'unforeseeable and retroactive judicial expansion of narrow and precise statutory language.'" Hussein, 351 F.3d at 14 (citation omitted); accord Balint, 201 F.3d at 935 (doctrine only applies if judicial interpretations "amount to an unpredictable shift in the law").

That doctrine does not apply here. The simplest reading of the statute is that the e-mail messages were "electronic communications" under the statute at the point where they were intercepted. One must apply tools of statutory construction to remove the conduct from the statute's ambit by interpreting a subtlety in the definition of "wire communications." Whatever else one might say about the Wiretap Act, "intercept[ing] . . . electronic communication[s]," 18 U.S.C. § 2511(1)(a), is "conduct that . . . the statute . . . has fairly disclosed to be within its scope," Lanier, 520 U.S. at 266.

Indeed, a 1997 law review article observed that, under a narrow interpretation of the ECPA's "intercept" prohibition, "unless some type of automatic routing software is used (for example, a duplicate of all an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of the ECPA is virtually impossible." Jarrod J. White, E-Mail @ Work.com: Employer Monitoring of Employee E-Mail, 48 Ala. L. Rev. 1079, 1083 (1997) (emphasis added); see also Pharmatrak, 329 F.3d at 22 (quoting this language approvingly). Thus, almost a year before Councilman's alleged conduct, the academic literature had noted that, even under a reading of the ECPA narrower than ours, "automatic routing software" that automatically forwarded duplicate copies of a user's

messages would qualify as "interception of E-mail within the prohibition of the ECPA." Id. That observation anticipated this case.[19]

III.

Although the text of the statute does not specify whether the term "electronic communication" includes communications in electronic storage, the legislative history of the ECPA indicates that Congress intended the term to be defined broadly. Furthermore, that history confirms that Congress did not intend, by including electronic storage within the definition of wire communications, to thereby exclude electronic storage from the definition of electronic communications.

We therefore conclude that the term "electronic communication" includes transient electronic storage that is intrinsic to the communication process, and hence that interception of an e-mail message in such storage is an offense under the Wiretap Act. Moreover, the various doctrines of fair warning do

[19]The dissent says that "White's article, like other scholarship available at the time, thus would have forcefully suggested that Councilman's conduct was not prohibited." Post at 51 (Torruella, J., dissenting). That is not so. Although the article described the implications of the Fifth Circuit opinion in Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 458 (5th Cir. 1994), it identified the possibility that, even under that case's narrow view of the intercept prohibition, there is a category of automatic e-mail routing software that might, in some situations, violate the Wiretap Act.

not bar prosecution for that offense. Consequently, the district court erred in dismissing the indictment.

Judgment vacated. Remanded for further proceedings consistent with this opinion.

- Dissenting Opinion Follows -

TORRUELLA, Circuit Judge, with whom CYR, Senior Circuit Judge, joins (Dissenting). Although I commend Judge Lipez on his erudite and articulate majority opinion, I am impeded from joining the same for two reasons. First, the indictment is legally insufficient to establish a criminal violation of 18 U.S.C. § 371 for conspiracy to violate the Wiretap Act, 18 U.S.C. § 2511, insofar as the e-mails Councilman is alleged to have retrieved were in "electronic storage," 18 U.S.C. § 2510(17), when that action took place, and therefore, the Wiretap Act's requisite element of "interception," 18 U.S.C. § 2511, is lacking. See United States v. Councilman, 373 F.3d 197, 200-04 (1st Cir. 2004). Second, and in the alternative, the result reached by the en banc majority deprives Councilman of due process of law, because he had no "fair warning" of the potential criminal consequences of his actions. See United States v. Lanier, 520 U.S. 259, 265 (1997).

But for the juxtaposition of our respective views, there is not much new in the positions of the majority and dissent from those presented by the panel opinion except that, by reason of the majority's conclusion that the indictment charges a valid criminal violation, we are required to discuss Councilman's due process claim, which the panel did not have to reach. See Councilman, 373 F.3d at 204 n.7.

I.

The facts of this case as stipulated by the parties state that "[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." (Emphasis added).

Stripped of all technical jargon, the sole legal issue presented by this appeal is whether the information contained in this computer system is data that can be "intercepted" within the meaning of the Wiretap Act. The answer to that question is not to be found in the wringing of the proverbial hands or dire warnings of the Doomsday that is predicted to follow one or the other conclusion. Cf. Yvette Joy Liebesman, The Potential Effects of United States v. Councilman on the Confidentiality of Attorney-Client E-Mail Communications, 18 Geog. J. Legal Ethics 893 (2005). Rather, the answer lies in a dispassionate reading of the legislation[20] upon which the criminal charges are based.

The statute that Councilman is charged with conspiring to violate provides for criminal sanctions against "any person who -- (a) intentionally intercepts,[21] endeavors to intercept, or procures

---

[20]As in the majority's opinion, statutory references herein are to the pre-2001 version of the Wiretap Act. See maj. op. at 6, n.4.

[21]The term "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

any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1) (emphasis added). The term "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 wire, radio, electromagnetic, photoelectronic or photooptical system." 18 U.S.C. § 2510(12). In contrast, the term "wire communication" is defined as "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[22] of such communication." 18 U.S.C. § 2510(1) (emphasis added).

It is Congress' failure to provide this emphasized language in its definition of "electronic communication" that incites the majority into engaging in what I believe to be an unfortunate act of judicial legislation that no amount of syllogization can camouflage. The lacuna between the definition of

---

other device." 18 U.S.C. § 2510(4).

[22]"Electronic storage" is broadly defined 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." 18 U.S.C. § 2510(17) (emphasis added).

"wire communication" and that of "electronic communication" can only be bridged by the body that created it; jurisprudential "body English" does not suffice to fill that vacuum. Although nature abhors a vacuum, it has no power over legislative oversights.

In finding the correct legal answer to the non-existent dilemma which the majority believes exists, we need go no further than our own In re Hart, in which, apropos of the present circumstances, we stated that, "[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." 328 F.3d 45, 49 (1st Cir. 2003) (quoting Barnhart v. Sigmon Coal Co., 534 U.S. 438, 452 (2002)). Contrary to the majority's assertions that this expressio unius presumption ought not apply because the language in question was not part of a "new, self-contained statute," maj. op. at 13, it is actually "made stronger when, as here, Congress has amended a statute to include certain language in some, but not all, provisions of the Statute." United States v. Steiger, 318 F.3d 1039, 1051 (11th Cir. 2003) (construing the Electronic Communications Privacy Act), cert. denied, 538 U.S. 1051 (2003); see also United States v. Fisher, 6 U.S. (2 Cranch) 358, 399 (1805) ("Where a law is plain and unambiguous, whether it be expressed in general or limited terms,

the legislature should be intended to mean what they have plainly expressed, and consequently no room is left for construction.").

These principles are particularly relevant to the interpretation of federal criminal statutes, for "[f]ederal crimes are defined by Congress, not the courts," and thus "policies of strict construction" should guide our actions. Lanier, 520 U.S. at 267 n.6.

It is not by coincidence that every court that has passed upon the issue before us has reached a conclusion opposite to that of the en banc majority: that the Wiretap Act's prohibition on intercepting electronic communications does not apply when they are contained in electronic storage, whether such storage occurs pre- or post-delivery, and even if the storage lasts only a few mili-seconds. See Theofel v. Farey-Jones, 359 F.3d 1066, 1077-78 (9th Cir. 2004) (post-delivery); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113-14 (3d Cir. 2003) (post-delivery); United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir. 2003) (on hard drive), cert. denied, 538 U.S. 1051 (2003); Konop v. Hawaiian Airlines, 302 F.3d 868, 878-79 (9th Cir. 2002) (on website server), cert. denied, 537 U.S. 1193 (2003); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461-62 (5th Cir. 1994) (pre-retrieval); see also United States v. Reyes, 922 F. Supp. 818, 836 (S.D.N.Y. 1996) (finding no interception where messages were retrieved from

pagers' memories prior to their retrieval by intended recipients because the messages were in "electronic storage").

Contrary to the en banc majority's view, our interpretation of the statute does not require that we assume that Congress contemplated the complete evisceration of the privacy protections for e-mail. When considering the intra-computer "interceptions" at issue here, Congress rationally may well have concluded that the public's privacy rights, or more specifically those between an e-mail service provider and its own customers, could be adequately controlled by normal contract principles rather than by federal statute. Councilman's "interception" of Interloc customers' e-mail was not akin to an interception engaged in by an outside party who was unrelated or unknown to the contracting parties. When a customer signs up with an e-mail provider like Interloc, he routinely is asked to read and expressly sign off on a privacy agreement which defines his expectations of privacy vis-à-vis the provider. If the protections are inadequate, he may decline the e-mail service and seek an alternative service contract which will afford him the protections he requires. Neither the Wiretap Act nor its legislative history forecloses the inference that Congress, in its exclusion of "electronic storage" from the definition of "electronic communication," intended to leave such matters to the exigencies of the contracting parties. If Interloc

did intercept its customers' messages in breach of a privacy agreement, the remedy lies in contract, not in the Wiretap Act.

I see no point in rummaging through the legislative history of a statute whose language, or more accurately, absence thereof, speaks for itself. "[W]hen the statute's language is plain, the sole function of the courts -- at least where the disposition required by the text is not absurd -- is to enforce it according to its terms." Dodd v. United States, 125 S. Ct. 2478, 2483 (2005) (quoting Hartford Underwriters Ins. Co. v. Union Planters Bank, N.A., 530 U.S. 1, 6 (2000)). This case presents the classic example of "legislative history [which] is itself often murky, ambiguous, and contradictory." Exxon Mobil Corp. v. Attapattah Servs., Inc., 125 S. Ct. 2611, 2626 (2005) (rev'g Rosario Ortega v. Star-Kist Foods, Inc., 370 F.3d 124 (1st Cir. 2004)).

> Judicial investigation of legislative history has a tendency to become, to borrow Judge Leventhal's memorable phrase, an exercise in 'looking over a crowd and picking out your friends.' . . . [J]udicial reliance on legislative materials like committee reports, which are not themselves subject to the requirements of Article I, may give unrepresentative committee members--or worse yet, unelected staffers and lobbyists--both the power and incentive to attempt strategic manipulations of legislative history to secure results they were unable to achieve through the statutory text.

Id. In any event, I refer to the panel opinion on this point. Councilman, 373 F.3d at 203-04.

I believe that both viewpoints on the first issue before the en banc court have been adequately expressed. Ultimately, it is up to the Supreme Court to determine which is correct, but, in my view the government has attempted to fish with a net that has holes in it and is thus in need of repair.

II.

Unfortunately, the matter does not end here. As demonstrated by the results of previous efforts by this and other courts to grapple with the statute in question, any lingering ambiguity that makes room for the majority's interpretation certainly qualifies as "grievous," maj. op. at 35. Due process, therefore, requires that the statute be construed against criminal liability, in accordance with the rule of lenity. See Lanier, 520 U.S. at 266; Huddleston v. United States, 415 U.S. 814, 831 (1974). Even if the ambiguity is not so serious, and "clarity at the requisite level may be supplied by [the majority's] judicial gloss on an otherwise uncertain statute, due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope." Lanier, 520 U.S. at 266. Whichever doctrine of "fair warning" one might apply, the bottom line is that the statute and the cases construing it did not make it "reasonably clear at the relevant time that the defendant's conduct was criminal." Id. at 267.

At the time that Councilman allegedly violated the Wiretap Act in 1998, he would have had available the following to guide his conduct: (1) the statute in question, and (2) the Jackson Games case (1994) and, tangentially, the Reyes case (1996). There is little in any of these that would have given Councilman fair notice of the en banc majority's interpretation, which itself requires reliance on legislative "history" that resembles a Byzantine maze.

Nor did the 1997 law review article cited by the majority render the interpretation adopted today foreseeable. Quite the opposite, in fact. That article examined the decision in Steve Jackson Games, 36 F.3d 457, in which the Fifth Circuit determined that the pre-retrieval seizure of private e-mails stored on a bulletin board server did not constitute an "intercept" under 18 U.S.C. § 2511(1)(a). White wrote:

> Rejecting the appellant's argument that logically seizure of something before it is received should constitute interception, the Steve Jackson Games court held that the E-mail stored on the [bulletin board's] computer hard drive was no longer in transmission, and thus could not be intercepted within the meaning of 18 U.S.C. S 2511(1)(a). . . . The narrowness of the Fifth Circuit's interpretation of "interception" is important. Following the Fifth Circuit's rationale, 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. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all an

> employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of the ECPA is virtually impossible.

White, supra, at 1082-83 (footnote omitted) (emphasis added). Clearly, the software used by Councilman was not "automatic routing software" that operates "before a newly composed message is saved to any temporary location." Id. at 1083. White's article, like other scholarship available at the time, thus would have forcefully suggested that Councilman's conduct was not prohibited. See Thomas R. Greenberg, E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute, 44 Am. U. L. Rev. 219, 249 (1994) ("Thus, the limitations imposed on employer interceptions of wire and electronic communications vanish once the same communication is in storage. Accordingly, in order to avoid Title III liability, an employer need only access employee communications once they have been stored."); Ruel Torres Hernández, ECPA and Online Computer Privacy, 41 Fed. Comm. L.J. 17, 39 (1988-1989) ("In other words, there simply is no ECPA violation if the person or entity providing a wire or electronic communication service intentionally examines everything [in storage] on the system, whether or not it is for the purpose of a quality control check.") (internal quotation marks omitted). Thus, I am at a loss to conceive how Councilman would have had fair notice of the majority's interpretation at the time of his actions.

Finally, Congress's provision of a good faith exception for those who divulge intercepted communications because they misconstrued the Wiretap Act's narrow exceptions to criminal liability as an affirmative defense, see maj. op. at 36-37 (citing 18 U.S.C. § 2520(d)(3)), is irrelevant. Councilman should not have to show he relied on those exceptions to divulge the e-mails he obtained, because he had no "reasonably clear" indication that to do so would otherwise violate the Wiretap Act.

Councilman is being held to a level of knowledge which would not be expected of any of the judges who have dealt with this problem, to say nothing of "men [and women] of common intelligence." Lanier, 520 U.S. at 266 (quoting Connally v. Gen. Constr. Co., 269 U.S. 385, 391 (1926)). If the issue presented be "garden-variety," maj. op. at 37 (quoting Sabetti v. Diapaolo, 16 F.3d 16, 18 (1st Cir. 1994)), this is a garden in need of a weed killer.

For the reasons stated, I respectfully dissent.