No. 03-1383

UNITED STATES OF AMERICA,
Appellant

v.

BRADFORD C. COUNCILMAN,
Appellee

On Appeal From A Judgment In A Criminal Case
Entered In The
United States District Court
For The District Of Massachusetts

PETITION OF THE UNITED STATES FOR REHEARING AND FOR REHEARING EN BANC

MICHAEL J. SULLIVAN
United States Attorney
District of Massachusetts

PAUL G. LEVENSON
GARY S. KATZMANN
Assistant U.S. Attorneys

PAUL K OHM
Trial Attorney
Computer Crime
and Intellectual Property Section,
Criminal Division, U.S. Department of Justice

JOEL GERSHOWITZ
JOHN A. DRENNAN
Attorneys, Appellate Section
Criminal Division, U.S. Department of Justice
950 Pennsylvania Avenue, N.W., Suite 1706
Washington, D.C. 20530
(202) 514-3622

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Rules

Miscellaneous

INTRODUCTION AND STATEMENT OF COUNSEL

An e-mail's path from sender to recipient is not direct. Like a pail of water moving from hand to hand as it travels from hose to flame in a bucket brigade, the e-mail is swiftly relayed from one computer to the next until it reaches the recipient. Intermediate computers store the electronic communication for only a small fraction of a second before they hand it off to the next computer in the chain. The Wiretap Act, 18 U.S.C. § 2510, et seq., as amended, protects the privacy of electronic communications by prohibiting their unlawful interception while traveling to the recipient. In a divided opinion, a panel of this Court held that this protection is intermittent; it stops and starts as the electronic communication is relayed from computer to computer. According to the panel majority, the statute does not prohibit the interception of the e-mail while it is stored momentarily in one of the intermediary computers. That holding squarely conflicts with another decision of this Court: In re Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003), and is incorrect. The Pharmatrak panel, unlike the majority in this case, held that the Wiretap Act bars the interception of all electronic communications that are "in transit" to their final destination, whether or not they are in temporary electronic storage at the moment of acquisition. 329 F.3d at 22. En banc review is thus necessary to reconcile these decisions. Because the panel's decision will undermine the privacy of e-mail

– a form of communication on which the public and commerce relies – this case also presents an issue of exceptional importance. See F. R. App. P. 36(a).

BACKGROUND

I. The Statutory Scheme

In 1968, Congress enacted the Wiretap Act, 18 U.S.C. § 2510 et seq., to protect the privacy of wire and oral communications. In 1986, the Electronic Communications Privacy Act (ECPA) amended the Wiretap Act to extend its privacy protections to electronic communications, such as e-mail and faxes. The Wiretap Act, as amended, makes it unlawful to intercept or to procure anyone else to intercept any oral, wire, or electronic communication (18 U.S.C. § 2511(1)(a)), or to use or disclose any illegally intercepted communication (18 U.S.C. § 2511(1)(c), (d)). "Intercept" is defined as the "acquisition of the contents of any wire, electronic, or oral communication through the use of [an] electronic * * * or other device." 18 U.S.C. § 2510(4).

The term "electronic communication" is defined in the Wiretap Act 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). The definition of "electronic communication" contains four express exclusions, such as wire and oral communications (e.g, phone calls), tone-only paging signals,

and certain stored "electronic funds transfer information." 18 U.S.C. § 2510(12). Communications in "electronic storage" are not among the stated exclusions.

Finally, under 18 U.S.C. § 2510(17), "electronic storage" is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," as well as the storage of such communication "by an electronic communication service for purposes of backup protection of such communication."[1]

II. The Charged Conduct And The Dismissal

According to the indictment, defendant ran an online rare and out-of-print book listing service called Interloc that provided customers with e-mail accounts. At defendant's direction, Interloc's chief technician reconfigured the mail processing software (procmail.rc) to make copies of all incoming messages from Amazon.com to Interloc's subscriber dealers. Interloc's computer system copied the messages during transmission – that is, before they were delivered to the recipient's e-mail in-boxes. Defendant

---

[1] As part of the ECPA, Congress also enacted the Stored Communications Act, 18 U.S.C. § 2701 et seq. That Act makes it unlawful for any individual intentionally and without authorization to access a facility through which an electronic communication service is provided and "thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701. The Stored Communications Act protects communications that are no longer in transit. For example, it covers a hacker who accesses and deletes stored e-mails.

and his employees read thousands of messages sent to its subscribers from Amazon in order to gain a competitive advantage. See United States v. Councilman, 373 F.3d 197, 199 (1st Cir. 2004).

Defendant was charged with conspiring to violate 18 U.S.C. § 2511 by intercepting electronic communications, disclosing intercepted communications, and using intercepted communications. On defendant's motion, the district court (Ponsor, D.J.) dismissed these charges on the ground that the e-mails in issue were in "electronic storage" at the time of their acquisition by defendant and therefore could not be "intercept[ed]" as a matter of law. See 373 F.3d at 199-200.

III. The Panel Opinions

A divided panel of this Court affirmed. The majority (Torruella, C.J., and Cyr, J.), held that the interception provisions of the Wiretap Act do not apply to electronic communications that are in temporary electronic storage, even if they are acquired in the course of transmission to the intended recipient. 373 F.3d at 203. The majority rested this conclusion on the fact that the definition of "wire communication" in the Act, 18 U.S.C. § 2510(1), explicitly includes communications in electronic storage while the definition of "electronic communication" does not. Id. at 200-201.[2] The majority concluded,

[2] Congress removed the reference to "electronic storage" from the definition of "wire communication" as part of the USA PATRIOT Act, P.L. 107-56 § 209, 115 Stat. 283 (2001).

based on the differing language in the two provisions, that Congress intended to give electronic communications "lesser protection" from surveillance than wire communications. Id. at 204. The majority acknowledged that, under its construction of the Act, much of the protection afforded by the Act to electronic communications may be "eviscerated." Id. at 203-204.

Judge Lipez dissented. Based on the statutory language and legislative history, he concluded that the Wiretap Act applies to the acquisition of electronic communications in transmission regardless of whether they are in temporary electronic storage. 373 F.2d at 209-212. Further, Judge Lipez regarded that conclusion as compelled by this Court's earlier decision in In re Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003). 373 F.3d at 214-215. Judge Lipez observed that, because electronic storage is an intrinsic aspect of the e-mail transmission process, the majority's approach would broadly deprive e-mail of the protection of the Wiretap Act, thereby "undo[ing] decades of practice and precedent regarding the scope of the Wiretap Act" and "essentially render[ing] the Act irrelevant to the protection of wire and electronic privacy." Id. at 219.

REASONS FOR GRANTING THE PETITION

All e-mail – indeed, any digital communication – continually moves in and out of electronic storage in the course of its transmission to its intended recipient. Such storage may last for

only a few nanoseconds. Yet here, the panel, prompting a strong dissent from Judge Lipez, held that e-mail in electronic storage during transmission is not protected by the Wiretap Act because it does not qualify as an "electronic communication" and thus cannot be "intercept[ed]" within the meaning of the Act. In other words, in the seconds in which e-mail makes its way from the sender to the recipient, its coverage by the Act depends on whether, at any given instant, it is in some form of momentary electronic storage.

The panel's decision merits further review for several reasons. First, it directly conflicts with this Court's decision in In re Pharmatrak, Inc., 329 F.3d 9 (2003), which holds that a communication acquired while en route to its intended recipient has been "intercept[ed]" within the meaning of the Wiretap Act regardless of whether it is temporarily in electronic storage at the moment of acquisition. Second, the panel's decision fails to recognize that the electronic storage of an e-mail during transmission is an indivisible component of the transmission. Third, the decision is inconsistent with the plain meaning of "intercept," which is to acquire a thing (such as a passed football) while it is en route to its intended destination. Fourth, the panel decision fails to recognize that the statutory definition of "electronic communication" contains several explicit exclusions, but none for communications in electronic storage generally. Finally, the decision contravenes the intent of

Congress to protect such communications. If allowed to stand, the decision, in the words of Judge Lipez, 373 F.3d at 219, will cause a "significant reduction" in the privacy of e-mail (and other forms of communication), because a large number of intrusions that would commonly be considered "intercept[ions]" will not be protected by the Wiretap Act.

I. The Panel's Decision Conflicts With This Court's Recent Decision In In re Pharmatrak, Inc.

In Pharmatrak, this Court made clear that the acquisition of an electronic communication while en route to the intended recipient qualifies as an "interception" regardless of whether the communication was acquired from temporary electronic storage.

Pharmatrak installed software on the computers of Internet users to track the websites they visited and to log the information they sent to those websites. Pharmatrak's software recorded the information contemporaneously with its transmission and sent the data to one of Pharmatrak's computers for processing. The captured information was either stored in RAM or in a user's computer hard drive when the program accessed it. 329 F.3d at 13-16; 373 F.3d at 214 (Lipez, J., dissenting).

This Court noted that some courts had distinguished, for purposes of deciding whether there had been an "interception" within the meaning of the Wiretap Act, between communications acquired in transit and those acquired from electronic storage

after transmission. 329 F.3d at 21. The Court observed that the "storage-transit" dichotomy was being outrun by technological developments, because "'[t]raveling the internet, electronic communications are often – perhaps constantly – both "in transit" and "in storage" simultaneously * * *.'" Id. at 21-22 (quoting United States v. Councilman, 245 F. Supp.2d 319, 321 (D. Mass. 2003)). The Court concluded, however, that it did not need to enter the debate over the existence of a "real-time requirement" because "[t]he acquisition by Pharmatrak was contemporaneous with transmission by the internet users * * *." 329 F.3d at 22. In other words, the Court held that, so long as the contemporaneity or "in transit" test is met, the "electronic storage" debate is irrelevant. Ibid. As in Pharmatrak, the communications in the instant case were in transit at the time they were acquired, so the result should be the same.

The panel attempted to distinguish Pharmatrak on the ground that the communications at issue there "were not placed in any type of storage before their interception." 373 F.3d at 201 n.6. But, as Judge Lipez explained, that conclusion is flatly incorrect: "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 out 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 * * *." 373 F.3d at 214 n.15. As Judge Lipez correctly concluded, the factual circumstances here are indistinguishable in any meaningful way from those in Pharmatrak, and "therefore, our conclusion that there was an interception in Pharmatrak should control our analysis here." Ibid.

It follows from the panel's reading of the Wiretap Act that, in the words of the panel itself, "Congress meant to give lesser protection to electronic communications than wire or oral communications." 373 F.3d at 203. But in Pharmatrak the Court stated that "ECPA amended the Federal Wiretap Act by extending to data and electronic transmissions the same protection already afforded to oral and wire communications." 329 F.3d at 18 (emphasis added). That statement is irreconcilable with the panel's view that Congress broadly intended to protect wire communications, but failed to protect electronic communications when (as invariably is the case) their transmission entails temporary, intermediate electronic storage.[3]

---

[3] In support of its holding, the panel majority cites two decisions from other circuits, Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994), and Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002). 373 F.3d at 202-203. But, as the panel itself acknowledged, "the electronic communications at issue here were acquired in a different manner than in [the cited cases]," because, unlike in those cases, "[d]efendant's procmail operated to obtain the e-mails before they were received by its intended recipients" – that is, while the e-mails "were being transmitted and in real time." Id. at 202-203 The type of temporary storage during transmission involved in the

II. The Panel's Construction Of The Wiretap Act Is Contrary To The Language And The Legislative History Of The Statute.

1. In Pharmatrak, the Court held that, even under the narrowest definition, an "intercept" occurs when one acquires an electronic communication contemporaneous with its transmission. 329 F.3d at 22. This is "consistent with the plain meaning of 'intercept,' which is 'to stop, seize, or interrupt in progress or course before arrival.'" Konop v. Hawaiian Airlines, 302 F.3d 868, 878 (9th Cir. 2002) (quoting Webster's Ninth New Collegiate Dictionary 630 (1985)). The e-mail at issue in this case, though in temporary electronic storage at the time of interception, was nevertheless in transit to the recipient, and thus was "intercepted" within the meaning of the Act.

The panel concluded that the interceptions were not prohibited by the Wiretap Act because the definition of "electronic communication" in the Act does not explicitly include communications in electronic storage. But the panel failed to recognize that the set of communications that is in electronic storage during transmission and the set that is "electronic communications" are not mutually exclusive – indeed, the statute plainly contemplates that what is in electronic storage is an "electronic communication." See 18 U.S.C. § 2510(17) (defining

---

instant case is "irrelevant to" the post-transmission storage involved in Jackson Games or the storage in a private secure website involved in Konop. 373 F.3d at 212 (Lipez, J., dissenting).

"electronic storage" as "storage of a wire or electronic communication * * *."). Moreover, as Judge Lipez reasoned, 373 F.3d at 209-210, the failure to explicitly include communications in electronic storage in the definition of "electronic communication" is less revealing of congressional intent than the fact that the definition does not explicitly exclude communications in electronic storage but does explicitly exclude four other categories of communication. See 18 U.S.C. § 2510(12). It is an established rule of statutory construction that "[w]here Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of contrary legislative intent." Andrus v. Glover Constr. Co. 446 U.S. 608, 616-617 (1980).

In concluding that the term "electronic communication" in the Wiretap Act does not reach communications in electronic storage during transmission, the panel reasoned that Congress must have intended to exclude them because, in the same legislation, it explicitly included "any electronic storage of such communication" in the definition of "wire communication." 18 U.S.C. § 2510(1). But, as Judge Lipez correctly observed, 373 F.3d at 210, the panel's reasoning "ignores the rationale behind Congress's inclusion of electronic storage in the definition of 'wire communication,'" which was to protect telephone calls while they were stored in voice mail – that is, after they were delivered. As

Judge Lipez concluded: "We should not misconstrue this easily understood inclusion of post-delivery voice mail storage as indicating an unstated intention to exclude emails in transmission from the scope of the Wiretap Act." Ibid.

2. The legislative history of ECPA supports the conclusion that, in expressly including within the definition of "wire communication" communications in electronic storage, Congress was extending the coverage of the Wiretap Act to non-contemporaneous acquisitions of wire communications (as from voice mail), and not limiting the protection of electronic transmissions, such as e-mails that have not yet reached their destination.

First, as Judge Lipez observed, 373 F.3d at 217, "virtually none of the discussions of electronic storage in House and Senate conference reports occur[s] within the context of message transmission or the Wiretap Act." If Congress had intended to significantly narrow the protection of electronic communications by excluding from the Act's coverage e-mail in electronic storage during transmission, "it would likely have discussed storage during transmission while it discussed the new provisions in the [Act]." Ibid. (Lipez, J., dissenting).

Second, the report of the House Committee on the Judiciary accompanying the ECPA states: "The contents of the voice portion of a wire communication in storage such as with 'voice mail' may not be obtained under [the Stored Communication Act]. [T]he provisions

of [the Wiretap Act] apply." H.R. Rep. No. 99-647, 99th Cong., 2d Sess., 67-68 (1986). Thus, it was Congress's intention, in defining "wire communication" to include communications in electronic storage, to extend the protections of the Wiretap Act beyond real-time transmissions to include voice mail, which remains in storage after the transmission is complete.

Finally, as both the majority and dissenting opinions recognize, electronic storage is a fundamental part of the e-mail transmission process. 373 F.3d at 199, 203; id. at 215 (Lipez, J., dissenting). Accordingly, if the Wiretap Act does not cover e-mail in electronic storage during transmission, the Act's protections against private and government surveillance of e-mail would, in the word of the panel itself, be "eviscerated." Contrary to the panel, it cannot avoid responsibility for this result by attributing this evisceration to developments in technology since the passage of the Act. Id. at 204. The technical specifications for e-mail transmission adopted by the group coordinating standards for the Internet in 1982 included a temporary storage component, and this specification was in use well before the enactment of the ECPA in 1986. See id. at 216 (Lipez, J., dissenting). Hence, the panel's construction of the statute would have rendered it a virtual nullity from the moment of its enactment.

III. The Issue Presented Is Exceptionally Important.

This decision is exceptionally important, warranting rehearing

en banc, because it would remove a large portion of real-time interceptions of e-mail from the coverage of the Wiretap Act. As a result, such e-mail would be covered solely by the Stored Communications Act, with its lesser protections. This means that Internet service providers would be free to access the private e-mail of their customers without criminal liability under either Act;[4] that criminals and corporate spies could monitor private e-mail without violating the Wiretap Act; and that the government would be able to gain access to e-mail in transit without following the Act's extra-constitutional strictures. Moreover, now that Congress has deleted from the definition of "wire communication" (see n.2, supra) communications that are in electronic storage, the government, under the panel's decision, could even eavesdrop on telephone calls (whenever digital transmission is involved) without running afoul of the Act.[5] Cf. 373 F.3d at 219 (noting parenthetically that "eighty percent of the telephone switches in the United States in 1991 were digital.") (citing United States

---

[4] See 18 U.S.C. § 2701(c)(I).

[5] Digital wire communications, such as digital telephone calls, are handed across networks in the same way as electronic communications. The voice signal is necessarily and momentarily placed in electronic storage at gateways, routers, hubs and other switching equipment as part of the transfer of the signal. See generally In re Matter of Federal-State Joint Board on Universal Service, 13 F.C.C.R. 11501, 11541-42 (Apr. 10, 1998). Thus, under the rule adopted by the panel, phone calls could be captured without violating the Wiretap Act, so long as eavesdroppers did so from one of several switches.

Congress, Office of Technology Assessment, Electronic Surveillance in a Digital Age 33 (1995)) (Lipez, J., dissenting). Given the drastic implications of the panel's decision, the Court should grant the instant petition.

CONCLUSION

This petition for rehearing and rehearing en banc should be granted.

Respectfully submitted,

MICHAEL J. SULLIVAN
United States Attorney

PAUL G. LEVENSON
GARY S. KATZMANN
Assistant U.S. Attorneys

PAUL K OHM
Trial Attorney
Computer Crime and
Intellectual Property Section
U.S. Department of Justice

_____

JOEL GERSHOWITZ
JOHN A. DRENNAN
Attorneys
Appellate Section
Criminal Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Suite 1706
Washington, D.C. 20530
(202) 514-3622

CERTIFICATE OF SERVICE

I hereby certify that I caused two copies of the foregoing Petition for Rehearing and for Rehearing En Banc to be served on August 27, 2004 by first-class mail on the appellee's attorney:

Andrew Good, Esq.
Good & Cormier
Attorneys-at-Law
83 Atlantic Avenue
Boston, Massachusetts 02110-3711

DINA MICHAEL CHAITOWITZ
Chief of Appeals
United States Attorney's Office

No. 03-1383

UNITED STATES OF AMERICA,
Appellant

v.

BRADFORD C. COUNCILMAN,
Appellee

Addendum Table of Contents