No. 07-56640

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

JUSTIN BUNNELL ET AL.,
Plaintiffs-Appellants,

v.

MOTION PICTURE ASSOCIATION OF AMERICA,
Defendant-Appellee.

On Appeal from Final Judgment of the
United States District Court for the Central District of California

The Honorable Florence Marie Cooper, United States District Judge
Case No. CV-06-03206-FMC

BRIEF FOR *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF PLAINTIFFS-APPELLANTS URGING REVERSAL OF THE DISTRICT COURT

MARC ROTENBERG
Counsel of Record
JOHN VERDI
Electronic Privacy Information Center
1718 Connecticut Ave., NW #200
Washington, DC 20009
(202) 483-1140

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, the Electronic Privacy Information Center ("EPIC") states that it is a 501(c)(3) non-profit corporation incorporated in the District of Columbia. EPIC has no parent corporation, and no publicly held company owns 10% or more of EPIC's stock.

STATEMENT OF *AMICUS*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC has participated as *amicus curiae* in numerous privacy cases. EPIC has a strong interest in this matter because interpretation of the Wiretap Act has a substantial impact on e-mail privacy rights.

EPIC files this *amicus curiae* brief with the consent of all parties.

SUMMARY OF ARGUMENT

The Wiretap Act's legislative history demonstrates that Congress intended to bar the interception of e-mail messages at all stages of the messages' transmittal. In doing so, the Wiretap Act provides some of the strongest protections for Americans' privacy.

The District Court's failure to find that Defendant-Appellee's actions violated the Wiretap Act is contrary to the Wiretap Act's legislative history, and threatens to strip citizens of vital privacy safeguards. If the Ninth Circuit Court of Appeals does not reverse the District Court's holding in this matter, Plaintiffs-Appellants will be wrongfully denied important privacy protections – protections that Congress intended to apply in these circumstances. Furthermore, failure to reverse would imperil the privacy rights of anyone who uses electronic mail.

ARGUMENT

I. AN E-MAIL CAN BE SIMULTANEOUSLY IN "ELECTRONIC STORAGE" AND SUBJECT TO INTERCEPTION UNDER THE WIRETAP ACT. THE EXCLUSION OF COMMUNICATIONS IN "ELECTRONIC STORAGE" FROM THE STATUTORY DEFINITION OF "ELECTRONIC COMMUNICATION" DOES NOT REFLECT A CONGRESSIONAL INTENT TO EXEMPT COMMUNICATIONS IN "ELECTRONIC STORAGE" FROM THE WIRETAP ACT.

The Defendant urges the Court to follow the basic reasoning of the District Court Opinion, which concludes that e-mails in "electronic storage," are not susceptible to interception under the Wiretap Act. See Bunnell v. Motion Picture Association of America, No. 03206 at 6-8 (C.D. Cal. August 22, 2007) (order granting defendant's motion for summary judgment). This theory has traditionally hinged on differences in the statutory definitions of "wire communication" and "electronic communication" to support the inference that the Wiretap Act does not protect electronic communications in "electronic storage." See United States v. Councilman, 373 F.3d 197, 201 (1st Cir. 2004), withdrawn, 385 F.3d 793 (1st Cir. 2004). According to the Defendant's theory, the absence of the phrase "electronic storage" in the definition of "electronic communication," when viewed in light of its inclusion in the definition of "wire communication," reflects an intention to exclude stored electronic communications from the Wiretap Act's protections.

This reading badly misconstrues the Electronic Communications Privacy Act's ("ECPA's") application to e-mail, and has been rejected by the First Circuit. See United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) (holding "the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process for [e-mail] communications."). ECPA's legislative history directly contradicts the Defendant's proposed analysis. In Councilman, the original sponsor of the Senate version of ECPA, Senator Patrick J. Leahy, filed an *amicus* brief stating:

> Congress intended for [the Wiretap Act] to protect electronic communications, like telephone calls, during the entirety of the transmission phase. ECPA's legislative history fully rebuts defendant's contention that electronic communications move in and out of Title III's umbrella depending on whether, at a precise moment in time, they are between or within the computers transmitting them to the user's mailbox.

United States v. Councilman, No. 03-1383 at 1-2 (1st Cir. November 12, 2004) (brief for Senator Patrick J. Leahy as *amicus curiae*).

Congress added "electronic storage" to the definition of wire communication not to *lessen* protections for stored e-mail, but rather to *expand* protections for one-time access to stored voicemail. Councilman, 418 F.3d at 76. The different treatment of stored communications reflects an effort to protect voicemail in effect from 1986 to 2001. During that period,

Congress extended the Wiretap Act to govern one-time accesses to stored voicemail as a stopgap measure to provide special privacy protections for voicemail. When this history is understood, it becomes clear that an electronic communication can be simultaneously in "electronic storage" and susceptible to interception under the Wiretap Act. The fact that the communications intercepted in this case were briefly in "electronic storage" tells us nothing about whether the Defendant's conduct violated the Wiretap Act.

To appreciate this point in greater detail, it helps to step back and recall Congress's basic goal of expanding the electronic privacy laws in light of technological change when it passed ECPA in 1986. By the mid 1980s, computer networks had created a new kind of private, non-voice communication susceptible to interception – electronic communications – and also introduced a new form of both wire and electronic communications – stored communications subject to one-time access. ECPA dealt with each development under different Titles of the Act. To protect ongoing and continuous accesses to the new communications, Title I of ECPA extended the highly protective Wiretap Act to computers; in the argot of the Wiretap Act, Congress added "electronic communications" where the law before had protected only "wire communications." Then, Congress regulated one-time

access to stored electronic communications by creating Title II of ECPA, the Stored Communications Act ("SCA"). The SCA is less protective of privacy than the Wiretap Act. See 18 U.S.C. §§ 2701-11.

These significant changes left a category unaddressed, however: they did not address how to regulate one-time access to stored wire communications such as voicemail. Voicemail was rare in 1986, but it did exist. See, e.g., United States v. Western Electric Co., 1986-1 Trade Cases P 66,987, 1986 WL 931 at *8 (D.D.C. 1986) (discussing voicemail). Congress could have protected voicemail under the modest protections of the SCA. After all, stored voicemail is conceptually similar to stored electronic communications such as e-mail: both are stored computer files held by a network service provider and retrieved at the user's request. However, Congress opted for a different approach that would confer higher protections on voicemail. Instead of expanding the SCA's relatively weak privacy protections to include voicemail, Congress limited the SCA to stored electronic communications, and conferred higher privacy protections for voicemail through other statutory means – the Wiretap Act.

Rather than create a new statute to protect voicemail, Congress took a simpler approach, and added just a few words to the Wiretap Act. Legislators amended the definition of wire communication by adding the

phrase "and such term includes any electronic storage of such communication." 18 U.S.C. § 2510(4) (1986), amended 2001. The Senate Report on ECPA explains the amendment and its intent:

> The Senate Judiciary Committee's Subcommittee on Patents, Copyrights and Trademarks amended [Section 101(a)(1)(D) of ECPA] to specify that wire communications in storage like voice mail, remain wire communications, *and are protected accordingly*.

S. Rep. No. 541, 99th Cong., 2d Sess. 1986, reprinted at 1986 U.S.C.C.A.N. 3555, 3566 (emphasis added). The phrase "electronic storage" was borrowed from 18 U.S.C. § 2510(17). Although its definition appears in Section 2510, the phrase was otherwise used only in the Stored Communications Act.[1]

As ECPA's legislative history demonstrates, Congress added "electronic storage" to the definition of wire communications in order to apply the Wiretap Act to circumstances involving criminal investigators who seek one-time access to stored voicemail. It is worth noting that this approach was well-intentioned, but not ideally crafted. The Wiretap Act was

---

[1]For historical reasons not relevant here, the definitions of statutory terms used by the Stored Communications Act appear in two places. Most of the terms appear in 18 U.S.C.§ 2510, along with other terms used by the Wiretap Act. Other terms appear in 18 U.S.C. § 2711, which until 2001 was the final section of the SCA. Section 2711(1) makes clear that terms defined in Section 2510 apply equally within the Stored Communications Act.

not designed to regulate one-time access; its mechanisms are best suited to ongoing acquisition. In addition, adding communications in storage to the definition of wire communication was textually redundant. Wire and electronic communications remain wire and electronic communications regardless of whether they are in transit or in electronic storage. Compare 18 U.S.C. § 2511 (1986) (protecting electronic communications in transit) with 18 U.S.C. § 2701 (1986) (protecting electronic communications in storage). Because "intercept" rather than "wire communication" or "electronic communication" defines the temporal scope of the Wiretap Act, the better approach may have been to define "intercept" in the case of wire communications so as to cover one-time access.

Whatever the technical merits of Congress's approach, the underlying goal motivating Congress's different treatment of wire and electronic communications is clear. Congress used different definitions to heighten protections for one-time access to stored wire communications under the Wiretap Act, not to exclude repeated intrusions on e-mail communications from the Act's privacy safeguards.

Recent federal legislation, including Section 209 of the USA PATRIOT Act of 2001 confirms this design. See Pub. L. 107-56, 115 Stat. 272, § 209. Section 209 temporarily undoes the 1986 treatment of voicemail

and instead grants stored voicemail the SCA's lesser protections. See *Let the Sun Set on PATRIOT - Section 209*, available at http://www.eff.org/Privacy/Surveillance/Terrorism/PATRIOT/sunset/209.php. The PATRIOT Act adds "wire communications" to the Stored Communications Act and removes the "electronic storage" clause from the definition of wire communication. See Pub. L. 107-56, 115 Stat. 272, § 209.[2] As this PATRIOT Act provision shows, the "electronic storage" clause in the definition of wire

---

[2] Section 209 states:

> **SEC. 209. SEIZURE OF VOICE-MAIL MESSAGES PURSUANT TO WARRANTS.** Title 18, United States Code, is amended--
>
> (1) in section 2510--
>
> (A) in paragraph (1), by striking beginning with `and such' and all that follows through `communication'; and
>
> (B) in paragraph (14), by inserting `wire or' after `transmission of'; and
>
> (2) in subsections (a) and (b) of section 2703--
>
> (A) by striking `CONTENTS OF ELECTRONIC' and inserting `CONTENTS OF WIRE OR ELECTRONIC' each place it appears;
>
> (B) by striking `contents of an electronic' and inserting `contents of a wire or electronic' each place it appears; and
>
> (C) by striking `any electronic' and inserting `any wire or electronic' each place it appears.

Section 209(1) removes the 1986 text designed to protect voicemail through the definition of "wire communication" in 18 U.S.C. § 2510(1); Section 209(2) adds "wire" to every mention of "electronic" communications in 18 U.S.C. § 2703.

communication and the absence of wire communications from the SCA from 1986 to 2001 are inextricably linked. The clause reflects Congress' intent, in passing ECPA, to extend the Wiretap Act to cover one-time access to voicemail, and to not exempt ongoing surveillance of temporarily stored e-mails from the Wiretap Act.

II. TO AVOID CONSTITUTIONAL DOUBT, THE COURT SHOULD CONSTRUE THE SCOPE OF THE WIRETAP ACT BASED ON THE CONSTITUTIONAL LINE DRAWN BY THE SUPREME COURT IN BERGER V. NEW YORK.

In Berger v. New York, 388 U.S. 41 (1967), the Supreme Court indicated that the Fourth Amendment triggers heightened scrutiny when surveillance is undertaken as "a series or a continuous surveillance" rather than as "one limited intrusion." Id. at 57. Under Berger, a statute that regulates "a series or a continuous surveillance" must include special privacy protections or risk facial invalidity under the Fourth Amendment. See id. at 56; see also Sibron v. New York, 292 U.S. 40, 59-60 (1968).

Congress enacted the Wiretap Act soon after Berger, and drafted the statute with Berger in mind. See Bartnicki v. Vopper, 532 U.S. 514, 522-23 (2001). The Wiretap Act's statutory framework was designed to satisfy the Fourth Amendment in the context of ongoing surveillance. Indeed, a number of circuit courts have indicated that the Wiretap Act's protections are required to ensure that ongoing surveillance satisfies the Fourth

Amendment even where the Act does not apply as a matter of statutory law. See, e.g., United States v. Torres, 751 F.2d 875, 885 (7th Cir. 1984) (Posner, J.) ("[W]e borrow the warrant procedure of [the Wiretap Act], a careful legislative attempt to solve a very similar problem, and hold that it provides the measure of the government's constitutional obligation of particular description in using television surveillance to investigate crime."); United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994) (citing cases from four circuits involving Fourth Amendment restrictions on video surveillance).

The fact that this case involves allegations of civil, rather than criminal, interception should make no difference. The Wiretap Act serves three functions at once. The same language: helps to define a code of criminal procedure, 18 U.S.C. § 2518; provides a civil remedy for private parties, 18 U.S.C. § 2520; and creates a substantive criminal prohibition, 18 U.S.C. § 2511. EPIC is aware of no authority suggesting that the Wiretap Act's key concepts should be interpreted differently in the civil context as opposed to the criminal context. An interpretation that applies in one context applies equally to other contexts. See, e.g., Campiti v. Walonis, 611 F.2d 387, 391-94 (1st Cir. 1979) (civil rights action citing civil and criminal Wiretap Act cases interchangeably).

The intimate relationship between the Wiretap Act and the Fourth Amendment should guide the Court here. The Court should construe the temporal aspect of "intercept" in 18 U.S.C. § 2510(4) to encompass "continuous surveillance" as contemplated by Berger. Any statutory ambiguity should be resolved to synchronize the scope of the Wiretap Act with the Fourth Amendment concerns that animate it. See United States v. Baranek, 903 F.2d 1068, 1072 (6th Cir. 1990) (noting the role of Fourth Amendment precedents in the proper interpretation of the Wiretap Act). Because the conduct in this case involved continuous, ongoing surveillance of the contents of electronic communications, the conduct constituted an "interception" under the Wiretap Act.

A less protective approach would raise grave constitutional concerns under Berger. The Supreme Court has explained that "where an otherwise acceptable construction of a statute would raise serious constitutional problems," courts should interpret statutory text "to avoid such problems unless such construction is plainly contrary to the intent of Congress." Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Constr. Trades Council, 485 U.S. 568, 575 (1988) (citing cases). Here, both the intent of Congress and constitutional considerations point in the same direction. They indicate that the Defendant intercepted e-mails in violation of the Wiretap

Act because he obtained their contents using a form of ongoing, continuous surveillance.

CONCLUSION

For the foregoing reasons, the judgment of the District Court should be reversed.

Respectfully submitted,

_____
MARC ROTENBERG
JOHN VERDI
Electronic Privacy Information Center
1718 Connecticut Ave., NW #200
Washington, DC 20009
(202) 483-1140

Dated: August 1, 2008

CERTIFICATE OF COMPLIANCE PURSUANT TO
FED. R. APP. P. 32(A)(7)(C) AND CIRCUIT RULE 32-1
FOR CASE NO. 07-56640

I certify that:

__ 1. Pursuant to Fed. R. App. P. 32 (a)(7)(C) and Ninth Circuit Rule 32-1, the attached opening/answering/reply/cross-appeal brief is

__ Proportionately spaced, has a typeface of 14 points or more and contains _____ words (opening, answering, and the second and third briefs filed in cross-appeals must not exceed 14,000 words; reply briefs must not exceed 7,000 words),
or is

__ Monospaced, has 10.5 or fewer characters per inch and contains _____ words or _____ lines of text (opening, answering, and the second and third briefs filed in cross-appeals must not exceed 14,000 words or 1,300 lines of text; reply briefs must not exceed 7,000 words or 650 lines of text).

__ 2. The attached brief is **not** subject to the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because

__ This brief complies with Fed. R. App. P. 32(a)(1)-(7) and is a principal brief of no more than 30 pages or a reply brief of no more than 15 pages;

__ This brief complies with a page or size-volume limitation established by separate court order dated _____ and is

__ Proportionately spaced, has a typeface of 14 points or more and contains _____ words,
or is

__ Monospaced, has 10.5 or fewer characters per inch and contains _____pages or_____ words or _____ lines of text.

__ 3. *Briefs in Capital Cases*

__ This brief is being filed in a capital case pursuant to the type-volume limitations set forth at Circuit Rule 32-4 and is

__ Proportionately spaced, has a typeface of 14 points or more and contains _____ words (opening, answering, and the second and third briefs filed in cross-appeals must not exceed 21,000 words; reply briefs must not exceed 9,800 words)
or is

__ Monospaced, has 10.5 or fewer characters per inch and contains _____ words or _____ lines of text (opening, answering, and the second and third briefs filed in cross-appeals must not exceed 75 pages or 1,950 lines of text; reply briefs must not exceed 35 pages or 910 lines of text).

_**X**_ 4. *Amicus Briefs*

_**X**_ Pursuant to Fed. R. App. P. 29(d) and 9th Cir. R. 32-1, the attached amicus brief is proportionally spaced, has a typeface of 14 points or more and contains 7000 words or less,
or is

__ Monospaced, has 10.5 or fewer characters per inch and contains not more than either 7000 words or 650 lines of text,
or is

__ Not subject to the type-volume limitations because it is an amicus brief of no more than 15 pages and complies with Fed. R. App. P. 32(a)(1)(5).

_____
JOHN VERDI
Attorney for:
Electronic Privacy Information Center
1718 Connecticut Ave., NW #200
Washington, DC 20009
(202) 483-1140

Dated: August 1, 2008

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that copies of the foregoing *amicus curiae* brief were this day sent by Federal Express to the office of the Clerk, and by U.S. Mail to counsel for the appellant and counsel for the appellee at the following addresses:

Ira P. Rothken
Rothken Law Firm LLP
3 Hamilton Landing
Suite 280
Novato, CA 94949
Counsel for Plaintiffs-Appellants

Ian H. Gershengorn
Steven B. Fabrizio
Jenner & Block LLP
1099 New York Avenue, N.W.
Suite 900
Washington, DC 20001-4412
Counsel for Defendant-Appellee

_____
JOHN VERDI
Attorney for:
Electronic Privacy Information Center
1718 Connecticut Ave., NW #200
Washington, DC 20009
(202) 483-1140

Dated: August 1, 2008