No. 03-1383

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

UNITED STATES,

Appellant,

v.

BRADFORD C. COUNCILMAN

Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR
THE DISTRICT OF MASSACHUSETTS

SUPPLEMENTAL BRIEF FOR THE CENTER FOR DEMOCRACY AND TECHNOLOGY, THE ELECTRONIC FRONTIER FOUNDATION, THE ELECTRONIC PRIVACY INFORMATION CENTER, THE AMERICAN LIBRARY ASSOCIATION, THE AMERICAN CIVIL LIBERTIES UNION, AND THE CENTER FOR NATIONAL SECURITY STUDIES AS AMICI CURIAE IN SUPPORT OF THE UNITED STATES IN FAVOR OF REVERSAL

ORIN S. KERR
George Washington University
Law School
2000 H Street, NW
Washington DC 20052
(202) 994-4775

(affiliation for identification
purposes only)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

CORPORATE DISCLOSURE STATEMENT

The Center for Democracy and Technology ("CDT") is a corporation with no parent corporation. No publicly held company owns 10% or more of the stock of CDT.

The Electronic Frontier Foundation ("EFF") is a corporation with no parent corporation. No publicly held company owns 10% or more of the stock of EFF.

The Electronic Privacy Information Center ("EPIC") is a corporation with no parent corporation. No publicly held company owns 10% or more of the stock of EPIC.

The American Library Association ("ALA") is a corporation with no parent corporation. No publicly held company owns 10% or more of the stock of ALA.

The American Civil Liberties Union ("ACLU") is a corporation with no parent corporation. No publicly held company owns 10% or more of the stock of ACLU.

The Center for National Security Studies ("CNSS") is a project of the National Security Archive Fund, Inc., a corporation with no parent corporation. No publicly held company owns 10% or more of the stock of the National Security Archive Fund, Inc.

STATEMENT OF AMICI

The Center for Democracy and Technology ("CDT") is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet and other communications networks. CDT represents the public's interest in an open, decentralized Internet reflecting constitutional and democratic values of free expression, privacy, and individual liberty.

The Electronic Frontier Foundation ("EFF") is a non-profit public interest organization, working through litigation and public education to secure civil liberties online and to support free expression and privacy in the digital world. Founded in 1990, EFF has over thirteen thousand members from across the United States and maintains one of the most linked-to Web sites in the world (http://www.eff.org).

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., that 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.

The American Library Association, founded in 1876, is the oldest and largest library association in the world. Its concerns span all types of

libraries: state, public, school, academic, and special libraries. With a membership of more than 64,000 librarians, library trustees, library educators, friends of libraries and other interested persons from every state, ALA is the chief advocate for the people of the United States in their search for the highest quality of library and information services.

Founded in 1920, the American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with approximately 400,000 members dedicated to the principles of liberty and equality embodied in the U.S. Constitution. The protection of principles of freedom of expression and privacy are areas of special concern to the ACLU. In this connection, the ACLU has been at the forefront in numerous state and federal cases involving emerging issues of freedom of expression and privacy.

The Center for National Security Studies ("CNSS") is a non-profit, public interest civil liberties organization founded in 1974 to ensure that civil liberties are not eroded in the name of national security. The Center has worked to protect the Fourth Amendment rights of Americans to be free of unreasonable searches and seizures, especially when conducted in the name of national security for more than twenty-five years.

ARGUMENT

I. 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." See 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). Its 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 Wiretap 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 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 "intercept" 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.

Amici recognize statements by some courts that the line between the Wiretap Act and the Stored Communications Act depends on whether communications are accessed in transit or when stored. See, e.g., Theofel v. Farey-Jones, 359 F.3d 1066, 1077-78 (9th Cir. 2003) (citing Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002)). This imprecise language should not be read as excluding ongoing surveillance of stored communications from the scope of the Wiretap Act. Every prior case on the line between the Wiretap Act and the Stored Communications Act involved a one-time access to a stored communication. In that factual context, the in-transit/in-storage distinction appeared to provide a convenient shorthand for the proper scope of the Wiretap Act. In cases involving one-time access, continuous surveillance and surveillance of a communication in transit seem

equivalent; if an acquisition occurs when a communication is actually moving, the surveillance must necessarily be ongoing and continuous. Similarly, a one-time access may seem synonymous with an access in storage; when a communication is stored, it typically will be obtained via a one-time access. The facts of this case expose why the in-transit/in-storage dichotomy is imprecise; it is technically possible to set up ongoing, continuous surveillance of communications when in instantaneous storage. While the in-transit/in-storage distinction provides an approximation that works for most cases, the more accurate line to be drawn is the continuous surveillance versus one-time access distinction drawn by the Supreme Court in Berger.

Finally, the fact that this case involves a criminal prosecution 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. *Amici* are aware of no cases suggesting that a key concept in the Wiretap Act should be interpreted differently depending on the context. As a result, 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).

II. 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 panel opinion, which concluded that e-mails in "electronic storage" could not be subject to interception under the Wiretap Act. See United States v. Councilman, 373 F.3d 197, 201 (1st Cir. 2004), withdrawn, 385 F.3d 793 (1st Cir. 2004). Under this theory, differences in the definition of wire and electronic communications compel the inference that the Wiretap Act does not protect electronic communications in "electronic storage." See id. at 201. Specifically, 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," is akin to the dog that did not bark. According to the Defendant, it reflects an intention to exclude stored electronic communications from the Wiretap Act's protections. Accord Councilman, 373 F.3d. at 201.

This reading badly misconstrues the Electronic Communications Privacy Act ("ECPA"), and it is important to understand exactly why. In brief, the reason is this: 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. 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. While this approach did blur the constitutional line drawn by Berger, it did so only to extend the Wiretap Act to govern one-time accesses in the special case of stored wire communications. When this history is understood, it becomes clear that an electronic communication can be simultaneously in "electronic storage" and subject to interception under the Wiretap Act. The fact that the communications intercepted in this case were in "electronic storage" tells us nothing about whether the Defendant's conduct violated the Wiretap Act.

To appreciate this difficult 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

communications not containing the human voice – 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 problem under different Titles of the Act. To protect ongoing and continuous accesses of the new communications, Title I of ECPA extended the high-protection Wiretap Act to computers; in the argot of the Wiretap Act, Congress added "electronic communications" where the law before had protected "wire communications." Then, to regulate one-time access to stored electronic communications such as e-mail, Title II of ECPA created the lower-protection Stored Communications Act ("SCA"), 18 U.S.C. § 2701-11.

These significant changes left a category open, 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). On one hand, Congress could have protected voicemail under the modest protections of the Stored Communications Act. After all, stored voicemail is conceptually similar to stored e-mail: it is a stored computer file held by a network service provider and retrieved at the user's request. Congress opted for a different approach

that would confer higher protections on voicemail. Instead of expanding the Stored Communications Act to include voicemail, Congress limited the SCA to e-mail and attempted to confer higher privacy protections for voicemail through other statutory means.

Rather than create a new statute to protect voicemail, Congress tried a simpler approach that added just a few words to the Wiretap Act. It 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]

---

[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

As this history explains, Congress added "electronic storage" to the definition of wire communications to require reliance on the Wiretap Act when criminal investigators sought a one-time access to stored voicemail. It is worth noting that this approach was well-intentioned but not ideally crafted. The Wiretap Act was not designed to regulate one-time access; its mechanisms are suited for 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 when stored). 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

---

Wiretap Act. Other terms appear in 18 U.S.C. § 2711, which until 2001 was the final section of the Stored Communications Act. Section 2711(1) makes clear that terms defined in Section 2510 apply equally within the Stored Communications Act.

communications is clear. Congress used different definitions to regulate one-time accesses of stored wire communications under the Wiretap Act, not to exclude repeated intrusions of stored electronic communications from the Act's protections.

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 protects stored voicemail under the lower protection Stored Communications Act. See *Let the Sun Set on PATRIOT - Section 209*, available at http://www.eff.org/Privacy/Surveillance/Terrorism/PATRIOT/sunset/209.php. It does so by simultaneously adding "wire communications" to the Stored Communications Act and removing the "electronic storage" clause from definition of wire communication. See Pub. L. 107-56, 115 Stat. 272, § 209.[2] As this provision of the Patriot Act suggests, the "electronic storage"

---

[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

clause in the definition of wire communication and the absence of wire communications from the SCA from 1986 to 2001 are inextricably linked. The clause reflects an effort to extend the Wiretap Act to cover one-time access to voicemail, not an effort to exempt ongoing surveillance of temporarily stored electronic communications from the Wiretap Act.

III. IT IS UNLIKELY THAT THE CONDUCT AT ISSUE IN THIS CASE VIOLATED THE STORED COMMUNICATIONS ACT.

This Court's *per curiam* order granting rehearing *en banc* posed a question for the parties to this case: "Whether the conduct at issue in this case could have been additionally, or alternatively, prosecuted under the Stored Communications Act?" United States v. Councilman, 385 F.3d 793

> (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.

(1st Cir. 2004). *Amici* submit that it is uncertain but unlikely that the conduct at issue violated the Stored Communications Act.

The only criminal provision of the Stored Communications Act is 18 U.S.C. § 2701. Section 2701 is a close cousin of the Computer Fraud and Abuse Act ("CFAA"), the federal computer hacking statute, codified at 18 U.S.C. § 1030. Like § 1030(a)(2), Section 2701(a) articulates a prohibition against accessing a computer without authorization, or exceeding authorization to that computer. The difference between § 1030(a)(2) and § 2701(a) is primarily jurisdictional; while § 1030(a)(2) applies to the broad category of all "protected computers," as defined in 18 U.S.C. § 1030(e)(2), Section 2701(a) applies only to the narrower class of "facilit[ies] through which an electronic communication service is provided," 18 U.S.C. § 2701(a)(1), as defined in 18 U.S.C. § 2510(15). In plain English, Section 1030 protects any computer connected to the Internet while Section 2701 only protects ISPs. [3]

[3] See generally Orin S. Kerr, A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1239-40 (2004) (contrasting Section 2701 with Section 1030(a)(2)); Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596 (2003) (hereinafter, Kerr, Cybercrime's Scope) (explaining the basic mechanisms of unauthorized access statutes such as the CFAA). Today, Section 2701 is largely redundant in light of the broad scope of Section 1030. This was not the case when Congress passed ECPA, however. At that

Any effort to prosecute Councilman under Section 2701(a) would encounter two major difficulties. First, it is unclear whether Councilman's conduct was "without authorization" or whether it exceeded authorization. As counsel for *amici* has explained in academic writing, the meaning of "authorization" in unauthorized access statutes is a topic of tremendous uncertainty. See Kerr, Cybercrime's Scope, supra note 3, at 1617-24, 1628-42.

Second, even if Councilman's conduct is without authorization or in excess of authorization, it likely would be exempt from liability under the exception codified at 18 U.S.C. § 2701(c)(1). This exception states that conduct authorized by "the person or entity providing a wire or electronic communication" is exempt from prosecution under Section 2701. This language was apparently intended to exempt ISPs and their employees from liability for looking through stored files stored on their own networks; it contrasts with a much narrower exception against criminal liability for analogous provider monitoring in the context of the Wiretap Act. See 18 U.S.C. § 2511(2)(a)(i). Although the exception likely applies here, its scope

---

time, the scope of the CFAA was quite narrow, as the CFAA applied only to "federal interest" computers. Congress dramatically expanded the CFAA's scope in 1994 and 1996, see United States v. Middleton, 231 F.3d 1207, 1211-12 (9th Cir. 2000), leading to the arguable redundancy that exists today.

remains uncertain. Of particular relevance in this case, it is unclear whether 2701(c)(1) implies an *ultra vires* exception such that an ISP employee acting without the official permission of the company would fall outside its terms. Is Councilman able to authorize his own conduct? If not, who can? At this point, the legal and factual uncertainties make it difficult to say.

Given the two legal hurdles that would need to be overcome to prosecute Councilman under Section 2701 of the Stored Communications Act, it seems uncertain but unlikely that a hypothetical prosecution under that Act would succeed.

CONCLUSION

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

Respectfully submitted,

_____
ORIN S. KERR
George Washington University
Law School
2000 H Street, NW
Washington, DC 20052
(202) 994-4775
First Circuit Bar No. 100530

Dated: November 12, 2004

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that copies of the foregoing amicus curiae brief was this day sent by Federal Express to the office of the Clerk, and by regular mail to counsel for the appellant and counsel for the appellee at the following addresses:

Joel Gershowitz
John A. Drennan
Appellate Section
Criminal Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

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

_____

ORIN S. KERR
George Washington University
Law School
2000 H Street, NW
Washington, DC 20052
(202) 994-4775

Dated: November 12, 2004