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

BRIEF FOR THE CENTER FOR DEMOCRACY AND TECHNOLOGY, THE ELECTRONIC FRONTIER FOUNDATION, THE ELECTRONIC PRIVACY INFORMATION CENTER AND THE AMERICAN LIBRARY ASSOCIATION AS AMICI CURIAE SUPPORTING APPELLANT'S PETITION FOR REHEARING AND REHEARING EN BANC

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

PETER P. SWIRE
Moritz College of Law, Ohio State University
55 West 12th Ave
Columbus, OH 43210
(240) 994-4142

(affiliation for identification purposes only)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

LEGISLATIVE MATERIALS

ARTICLES

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.

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 ("ALA"), 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.

SUMMARY OF ARGUMENT

This case has repercussions far beyond a single criminal prosecution. The panel opinion effectively rewrites the field of Internet surveillance law in ways that no one in Congress ever imagined. As the *New York Times* editorial on the case demonstrates, the panel opinion has dramatic and disturbing implications for Internet privacy. The opinion also raises profound constitutional questions by unhinging the Wiretap Act from the Fourth Amendment decision it codifies, Berger v. New York, 388 U.S. 41 (1967). The panel's statutory construction may render portions of the Internet surveillance statutes facially unconstitutional. The petition for rehearing or rehearing en banc should be granted.

ARGUMENT

I. THE PANEL OPINION EFFECTIVELY REWRITES THE FIELD OF INTERNET SURVEILLANCE LAW ALONG PRINCIPLES NEITHER CONGRESS, THE JUSTICE DEPARTMENT, PRIVACY GROUPS, NOR THE SCHOLARLY COMMUNITY HAS EVER IMAGINED.

The Wiretap Act is largely an attempt to codify the Supreme Court's Fourth

Amendment decision in Berger v. New York, 388 U.S. 41 (1967). See Mitchell v. Forsythe, 472 U.S. 511, 532 (1985). In Berger, 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 388 U.S. at 57. The meaning of "intercept" in 18 U.S.C. § 2510(4) traditionally has been viewed in light of that history. It has been widely understood that whenever a person intercepts the contents of Internet communications through mechanisms that are "the equivalent of a series of intrusions," Berger, 388 U.S. at 59, such an intercept triggers the Wiretap Act.

The panel opinion unhinged the Wiretap Act from Berger. It looked not to whether the intrusion was a one-time event or a series of intrusions, but rather to whether the data was moving or still at the precise nanosecond it was obtained. See United States v. Councilman, 373 F.3d 197, 203 (1st Cir. 2004). According to Judges Torruella and Cyr, the instant that a communication comes to rest it somehow falls outside the scope of the Wiretap Act's protections – no matter how briefly the communication is at rest. See id.

This approach rewrites the basic principles of Internet surveillance law. While this case happens to involve a criminal prosecution for illegal wiretapping, the Wiretap Act functions primarily as a code of criminal procedure. The Wiretap Act is the primary source of legal protections against government snooping online.

The panel's approach guts those protections. It would allow federal, state, or local law enforcement agents to install monitoring devices that impose the functional equivalent of a wiretap without needing to satisfy the Wiretap Act. Because many surveillance devices can be installed in a way that obtains communications while in nanosecond storage, the panel opinion threatens to reduce the Wiretap Act to almost a nullity.

Congress plainly did not intend such a result. When Congress passed the Electronic Communications Privacy Act ("ECPA") in 1986 to protect the privacy of e-mail, it followed the constitutional teachings of Berger. The Wiretap Act was extended to the Internet to regulate continuous intrusions over a period of time. See, e.g., 18 U.S.C. § 2518(1)(d). The Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-11, was created to provide rules for the one-time disclosure of private information. See 18 U.S.C. § 2703(a). By focusing on the velocity of the communication instead of Berger's constitutional line, the panel opinion largely nullified a statute that Congress has relied upon to protect e-mail privacy for almost two decades.

Senator Patrick Leahy, one of the key figures behind ECPA in 1986, recently made this precise point on the floor of the Senate in response to the panel opinion:

> The 2-to-1 decision by the First Circuit Court of Appeals in a case called United States v. Councilman has dealt a serious blow to online privacy. . . . If allowed to stand, this decision threatens to eviscerate Congress's careful efforts to ensure that privacy is protected in the modern information age.
>
> . . . .
>
> ECPA was a careful, bipartisan and long-planned effort to protect electronic communications in two forms--from real-time monitoring or interception as they were being delivered, and from searches when they were stored in record systems. We recognized these as different functions and set rules for each based on the relevant privacy expectations and threats to privacy implicated by the different forms of surveillance.
>
> The Councilman decision turned this distinction on its head.

Cong. Rec. S7893-96 (daily ed. July 9, 2004) (statement of Sen. Leahy). As Senator Leahy's comment makes clear, the panel's reading of the Act creates a remarkable statutory hole.

The panel opinion explains away this bizarre result by suggesting that Congress is somehow at fault; it suggests that the text of the Wiretap Act "may be out of step with the technological realities of computer crimes." Councilman, 373 F.3d at 204. But this argument makes little sense. E-mail works basically the same way today as it did in 1986, the year Congress passed the Electronic Communications Privacy Act ("ECPA") with the specific goal of protecting the privacy of e-mail. See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848. Although many other Internet applications have advanced substantially since 1986, as a technological matter e-mail has changed very little.

The panel opinion creates an illogical distinction that dramatically weakens the Wiretap Act to the detriment of every American who uses e-mail. See Intercepting E-Mail, N.Y. Times, July 2, 2004 at A18. Its approach has no basis in the text, purpose, or history of the surveillance laws.

II. THE PANEL OPINION RAISES GRAVE CONSTITUTIONAL DIFFICULTIES BY UNHINGING THE WIRETAP ACT FROM THE FOURTH AMENDMENT PRINCIPLES ANNOUNCED BY THE SUPREME COURT IN BERGER v. NEW YORK.

By de-linking the Wiretap Act from the Berger decision, the panel opinion also raises important and difficult constitutional problems. According to Berger, the Fourth Amendment requires that a wiretapping regime must satisfy specific constitutional requirements. See Berger, 388 U.S. at 56. If the statutory law regulating the issuance of warrants and court orders to allow monitoring does not provide sufficient protection, that law may be subject to facial challenge. See Sibron v. New York, 292 U.S. 40, 59-60 (1968).

The panel opinion's statutory interpretation may render the Stored Communications Act facially unconstitutional under this standard. Under the panel opinion, a significant proportion of wiretapping practices thought to be regulated by the Wiretap Act actually are governed only by the Stored Communications Act. The Stored Communications Act does not offer the kind of privacy protection that the Fourth Amendment requires under Berger, however.

See generally Berger, 388 U.S. at 58-60 (articulating Fourth Amendment requirements for a statute that permits wiretapping). Like the statute invalidated in Berger, the Stored Communications Act does not require that the order allowing the wiretapping name the specific crime that is under investigation, or guarantee that the wiretapping will occur only for a short period of time. Compare Berger, 388 U.S. at 58-60 with 18 U.S.C. § 2703. Similarly, the SCA "has no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts. On the contrary, it permits unconsented entry without any showing of exigent circumstances." Berger, 388 U.S. at 60.

The SCA has the same defects that the Supreme Court used as a basis to invalidate the New York wiretapping statute in Berger. There is a simple reason for that, of course: Congress never intended the Stored Communications Act to govern ongoing surveillance. But the panel opinion's approach requires it to shoulder these burdens. Its holding that the e-mails at issue were in "electronic storage" means not only that ISPs are free to monitor their customer's email for their own competitive advantage, as occurred in this case, but also that the government could compel a provider to obtain and disclose such e-mails under Section 2703 of the SCA, not the Wiretap Act. By pushing ongoing surveillance out of the Wiretap Act and into the SCA, the panel opinion may render the SCA facially unconstitutional under Berger.

CONCLUSION

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

Respectfully submitted,

_____

ORIN S. KERR[1]
George Washington University
Law School
2000 H Street, NW
Washington, DC 20052
(202) 994-4775

PETER P. SWIRE
Moritz College of Law
Ohio State University
55 West 12th Ave
Columbus, OH 43210
(240) 994-4142

(affiliation for identification purposes only)

Dated: September 2, 2004

[1] Application for Admission to Practice before the First Circuit pending.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that two copies of the foregoing amicus curiae brief and motion for leave to file were this day sent 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: September 2, 2004