No. 06-4092

IN THE UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

STEVEN WARSHAK,

Plaintiff-Appellee,

v.

UNITED STATES OF AMERICA,

Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF OHIO AT CINCINNATI

BRIEF FOR PROFESSORS OF ELECTRONIC PRIVACY LAW AND INTERNET LAW AS *AMICI CURIAE* OPPOSING THE PETITION OF THE UNITED STATES FOR REHEARING EN BANC

PATRICIA L. BELLIA
Notre Dame Law School
P.O. Box 780
Notre Dame, IN 46556
(574) 631-3866

SUSAN FREIWALD
University of San Francisco School of Law
2130 Fulton Street
San Francisco, CA 94117
(415) 422-6467

(affiliations for identification purposes only)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Legislative Materials

INTEREST OF AMICI

Amici are scholars who teach, write about, or have an interest in electronic privacy law and Internet law. *Amici* have no stake in the outcome of this case, but are interested in ensuring that electronic privacy law develops with due regard for the vital role electronic communications play in our lives. A full list of *amici* is appended to the signature page. The United States has consented to the filing of this brief. Warshak has informed us that he assents to the filing of this brief to the extent the Court is considering *en banc* review for reasons other than the procedural issues raised by government's petition, but for reasons previously stated he respectfully contends that that the procedural issues raised in the government's petition do not warrant *en banc* review.

SUMMARY OF ARGUMENT

En banc review of a panel decision is an extraordinary step, generally taken only when a panel decision conflicts with a decision of the U.S. Supreme Court, with the court's own precedent, or with decisions of other Courts of Appeals, or when the underlying question is one of exceptional importance. Fed. R. App. P. 35(b)(1). The Government claims that the panel's decision satisfies these criteria. Although it focuses on procedural issues, the Government also strongly implies that the panel's ruling on the applicability of the Fourth Amendment to electronic communications itself provides a basis for *en banc* review. In particular, the Government suggests that the panel erred in concluding that users generally have an expectation of privacy in their stored electronic communications. *See* Petition of the United States for Rehearing En Banc, *Warshak v. United States*, No. 06-4092, at 2, 13-15 (6th Cir. filed Aug. 1, 2007) ("Government Petition"). As demonstrated below, however, the panel's approach to the underlying Fourth Amendment question conforms to all applicable Supreme Court precedents and creates no conflict with other Court of Appeals decisions. Moreover, the Government's suggestion that the panel's partial invalidation of the Stored Communications Act will disrupt decades-old investigative practices supported by a carefully crafted congressional scheme is as irrelevant as it is overstated.

In short, the panel's resolution of the underlying Fourth Amendment claim presents no issues worthy of *en banc* review.[1]

ARGUMENT

I. THE PANEL'S CONSTITUTIONAL REVIEW OF THE GOVERNMENT'S SURVEILLANCE PRACTICES CONFORMED TO ALL APPLICABLE PRECEDENTS

Under foundational constitutional principles, courts must ensure that executive branch surveillance practices satisfy Fourth Amendment prerequisites. The panel did just that when it found that a law enforcement demand for e-mails stored with service providers generally constitutes a Fourth Amendment search. It appropriately required law enforcement agents to obtain a warrant based on probable cause unless they can convince a judge that the user lacks a reasonable expectation of privacy in the e-mails they seek. The judiciary must oversee executive branch demands for information that implicate the Fourth Amendment. To do otherwise, as the Government requests, would sanction executive branch overreaching and render constitutional protections a nullity.

Having found e-mail subject to users' reasonable expectations of privacy, the panel imposed standard Fourth Amendment procedural requirements on law enforcement access to it. Accordingly, the panel declared unconstitutional certain provisions in the Stored Communications Act, 18 U.S.C. §§ 2701-2709, 2711-2712

[1] We do not address the procedural issues raised by the Government's petition.

("SCA"), to the extent they authorized the government to evade those requirements. In doing so, the panel proceeded exactly as the Supreme Court did in *Berger v. New York*, 388 U.S. 41 (1967), when it declared unconstitutional a New York statute that did not impose adequate Fourth Amendment safeguards on law enforcement eavesdropping. No case has cast doubt on the Supreme Court's constitutional interpretation in *Berger*. In fact, a year after *Berger*, Congress incorporated all of the decision's procedural safeguards into the Wiretap Act.[2] *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9 (2004).

The panel also followed settled Supreme Court law when it used the reasonable expectations of privacy test to resolve the Fourth Amendment question. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The Supreme Court has frequently sanctioned that approach to questions of constitutional privacy. *See Kyllo v. United States*, 533 U.S. 27, 32-33 (2001). The panel found e-mails subject to a reasonable expectation of privacy, just as the Supreme Court in *Katz* had found telephone conversations to be. *Warshak v.*

[2] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Title III, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2522 (2000 & Supp. IV 2004)). That there are not more cases in the *Berger* line does not undermine the Court's approach in that case. Congress' nearly immediate codification of the constitutional requirements enunciated in *Berger* made it possible to test law enforcement practices against the federal Wiretap Act and analogous state statutes and thereby avoid unnecessary constitutional analysis.

United States, 490 F.3d 455, 469-76 (6th Cir. 2007). Because e-mail is the modern analogue to the telephone, and because both play a vital role in private communication, *id.* at 473, the panel's decision should not surprise anyone familiar with modern communications.

Neither *Smith v. Maryland*, 442 U.S. 735 (1979), nor *United States v. Miller*, 425 U.S. 435 (1976), counsels a different result. *Smith* does not apply, as the panel recognized, because it considered dialed telephone numbers, and not the contents of telephone calls or e-mails. As for *Miller*, the panel found it controlling in two factual situations. First, when a user sends an e-mail directly to her service provider, the provider may disclose that e-mail correspondence without the user's consent. *Warshak*, 490 F.3d at 475. Second, when a provider's employees regularly access the contents of a user's e-mails in the ordinary course of their business, and the user is aware of that total access, the user retains no reasonable expectation that the provider will respect the privacy of those e-mails. *Id.* at 473-74. In both situations, the panel applied *Miller*'s assumption-of-risk analysis to find that an e-mail user has no constitutional complaint when someone to whom she has given total access to her communications discloses them to the government.

Contrary to the Government's suggestions, *see* Government Petition at 13, *Miller* does not govern those communications a user stores with a third party but to

which she provides limited rather than total access. The panel identified several situations in which users provide a third party with limited access to their information or effects and do not thereby waive their reasonable expectations of privacy. *Katz*, for one, established that users maintain a reasonable expectation of privacy in their telephone calls, despite telephone employees' technical ability to monitor those communications. *Katz*, 389 U.S. at 353.

The panel also found analogous the storage of possessions in safe deposit boxes or storage lockers. *Warshak*, 490 F.3d at 470-72. In both cases, the user maintains a reasonable expectation of privacy, despite the fact that she has placed her possessions in another's hands for safekeeping and provided limited access thereto. *See United States v. Johns*, 851 F.2d 1131, 1135-36 (9th Cir. 1988) (implicitly recognizing reasonable expectation of privacy in rented storage unit); *see also Stoner v. California*, 376 U.S. 483, 489-90 (1964) (search of hotel room without warrant violated Fourth Amendment, even though one who engages a hotel room implicitly permits hotel personnel to enter it to perform their duties).

The principle that users may entrust their communications to others without waiving their constitutional privacy goes back at least as far as *Ex parte Jackson*, 96 U.S. 727, 733 (1878). In that case, the Supreme Court found that postal employees' handling of personal letters did not permit law enforcement agents to demand letters from them without first obtaining a warrant based on probable

cause. *Id.* at 733. The Supreme Court reaffirmed that principle in *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."); *see also United States v. Long*, 64 M.J. 57, 63 (C.A.A.F. 2006) (consent to monitoring did not imply consent to "engage in law enforcement intrusions by examining the contents of particular e-mails in a manner unrelated to the maintenance of the e-mail system").

It is simply not the case that the panel overturned settled law; indeed, this case falls directly in line with the only two decisions on point—i.e., the decisions of the Court of Appeals for the Armed Forces in *Long*, 64 M.J. at 57, and *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996).

By translating the reasonable expectation of privacy into the language of electronic communications, the court provided much needed clarity. Its decision conforms to applicable precedents and presents no basis for reconsideration.

II. THE PANEL PROPERLY STRUCK DOWN UNCONSTITUTIONAL APPLICATIONS OF THE STORED COMMUNICATIONS ACT

The Government suggests that the panel's decision disrupts longstanding government investigative practices by invalidating portions of the Stored Communications Act that have been on the books for twenty years. The judiciary has an obligation to strike down statutory provisions that authorize unconstitutional

practices, and may not sanction constitutional violations while it waits for Congress to get it right. The suggestion that the panel somehow overstepped its bounds by determining the constitutionality of the government's investigative methods misconstrues the basic principle of judicial review.

That the panel addressed the Fourth Amendment's application to e-mail twenty years after passage of the SCA should cast no doubt on the decision. *Berger* and *Katz* established Fourth Amendment protection for telephone calls nearly a century after the invention of the telephone. The Supreme Court struck down a different provision of the federal surveillance laws almost seventy years after such provision had been in place. *See Bartnicki v. Vopper*, 532 U.S. 514, 517 (2001) (finding unconstitutional a disclosure prohibition that had been part of federal law since 1934).

Even if Congress's judgments about the constitutionality of certain surveillance practices were entitled to deference, deference is entirely inappropriate in this context for two reasons. First, the suggestion that Congress in fact perceived law enforcement agents' acquisition of stored e-mail without a warrant to be constitutional rests on a highly contested interpretation of the SCA.[3] The

[3] More precisely, it depends on reading the SCA to exclude e-mails already accessed by a subscriber from "electronic storage," and thus from the warrant-level protection of § 2703(a) of the SCA. Courts are divided on how to apply the term "electronic storage" to e-mails already accessed by a subscriber. *Compare Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir.) (concluding that opened e-mails are

legislative reports accompanying the SCA themselves indicate conflicting views on whether stored e-mail is entitled to Fourth Amendment protection.[4]

Second, even if the Government could establish that Congress concluded that stored e-mails were unprotected by the warrant requirement of the Fourth Amendment, there are good reasons not to defer to any judgment Congress (is claimed to have) made in 1986. When Congress passed the SCA, e-mail as we know it today did not exist. Commercial e-mail providers primarily served the business community. *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1557 (2004). E-mail had to be actively moved into storage to be stored indefinitely. *See id.* at 1569. Today, e-mail is often stored indefinitely with a service provider when the subscriber simply chooses not to delete it. In short, because Congress could not have foreseen the range of circumstances in which e-mail is used, any conclusion it

---

in "electronic storage"), *cert. denied*, 543 U.S. 813 (2004), *with Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) (finding e-mails in post-transmission storage not in "electronic storage"), *aff'd in part on other grounds*, 352 F.3d 107, 114 (3d Cir. 2004).

[4] *Compare* S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 (expressing fear that communications in hands of service providers "may be subject to no constitutional privacy protection") *with* H.R. REP. NO. 99-647, at 22 (1986) ("It appears likely . . . that the courts would find that the parties to an e-mail transmission have a 'reasonable expectation of privacy' and that a warrant of some kind is required.") *and id.* at 23 (suggesting that the contents of some electronic communications in storage enjoy a higher degree of Fourth Amendment protection than customer records).

(is claimed to have) reached about the availability of Fourth Amendment protection for e-mail in 1986 is not particularly informative.

The Government's complaint that the panel's decision overturns twenty years of government practice, Government Petition at 1, likewise should be accorded no weight. The Supreme Court recognized in *Berger* that it "could not forgive the requirements of the Fourth Amendment in the name of law enforcement," *Berger*, 388 U.S. at 62.

There is also reason to be skeptical about the Government's assertions with respect to the scope and relevance of its practices over the last two decades. As noted above, at the time the SCA was adopted, the Internet was simply not widely used as a medium for personal communications. It is only in the last several years that long-term storage of e-mails with third-party service providers has become commonplace, and thus that a large pool of e-mails already accessed by the subscriber has become available for government investigations. Moreover, the ability to challenge such practices depends on the government providing notice of them. In a case where the Government has confessed error for its failure to provide notice in compliance with the statute (and, indeed, the magistrate's order), it would be particularly ironic to use executive branch "practice" as the measure of constitutional legitimacy. That the government has consistently violated the

constitutional privacy of e-mail users and would like to persist in those practices further buttresses the need for the panel's clear statement of constitutional law.

The panel's decision places no burden on law enforcement agents other than that they respect constitutional rights. In contemplating that law enforcement agents either obtain a warrant and satisfy Fourth Amendment prerequisites, or refute the user's Fourth Amendment claims before a court, the panel simply requires a member of the judiciary to agree that the user lacks a reasonable expectation of privacy in the targeted e-mails. The Constitution requires no less. *United States v. United States Dist. Ct.*, 407 U.S. 297, 317 (1972) ("The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.").

CONCLUSION

In sum, the panel's resolution of Warshak's underlying Fourth Amendment claim provides no basis for *en banc* review.

Respectfully submitted,

_____

PATRICIA L. BELLIA
Notre Dame Law School
Notre Dame, In 46556
(574) 631-3866

SUSAN FREIWALD
University of San Francisco School of Law
2130 Fulton Street
San Francisco, CA 94117
(415) 422-6467

Counsel for Amici Curiae

Dated: September 5, 2007

APPENDIX – LIST OF AMICI[1]

John B. Anderson
Distinguished Visiting Professor of Law
Shepard Broad Law Center
Nova Southeastern University
formerly Representative, United States Congress (R-Ill.) (1961-1981)

Patricia L. Bellia
John Cardinal O'Hara, C.S.C. Associate Professor of Law
Notre Dame Law School

Ralph D. Clifford
Associate Dean & Professor of Law
Southern New England School of Law

Susan Freiwald
Professor of Law
University of San Francisco School of Law

Eric Goldman
Assistant Professor of Law
Academic Director, High Tech Law Institute
Santa Clara University School of Law

Stephen E. Henderson
Associate Professor of Law
Widener University School of Law

William J. Luddy, Jr.
Clinical Professor of Management
Lally School of Management & Technology
Rensselaer Polytechnic Institute

[1] Affiliations for identification purposes only.

Deirdre K. Mulligan
Clinical Professor of Law
Director, Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley
School of Law – Boalt Hall

Malla Pollack
Professor of Law
American Justice School of Law

Neil M. Richards
Associate Professor of Law
Washington University in St. Louis

Michael L. Rustad
Thomas F. Lambert Jr. Professor of Law
and Co-Director of Intellectual Property Law Program
Suffolk University Law School

Pamela Samuelson
Richard M. Sherman Distinguished Professor of Law & Information
University of California, Berkeley

Wendy Seltzer
Visiting Assistant Professor of Law
Northeastern University School of Law

Christopher Slobogin
Stephen C. O'Connell, Chair, Professor of Law
University of Florida College of Law

Katherine J. Strandburg
Visiting Professor
New York University School of Law
Associate Professor of Law
DePaul University College of Law

Peter Swire
C. William O'Neill Professor of Law
Moritz College of Law of the Ohio State University
formerly Chief Counselor for Privacy, U.S. Office of Management and Budget (1999-2001)

Mary W.S. Wong
Professor of Law
Franklin Pierce Law Center

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing brief complies with the type-volume limitation provided in Rule 32(a)(7)(C)(i) of the Federal Rules of Appellate Procedure. This brief contains 2,330 words of Times New Roman (14 point) proportional type and was prepared using Microsoft Word.

PATRICIA L. BELLIA
Notre Dame Law School
Notre Dame, IN 46556
(574) 631-3866

CERTIFICATE OF SERVICE

I hereby certify that the foregoing Brief for Professors of Electronic Privacy Law and Internet Law as *Amici Curiae* Opposing the Petition of the United States for Rehearing *En Banc* was served this 5th day of September, 2007, by first-class mail to counsel listed below, and that, pursuant to Fed. R. App. P. 25(a)(2)(B)(i), said brief was filed by dispatching an original and twenty-five paper copies via express courier to the Clerk of the Court.

GREGORY G. LOCKHART
United States Attorney
DONETTA D. WIETHE
BENJAMIN C. GLASSMAN
Assistant U.S. Attorneys
221 E. 4th St., Ste. 400
Cincinnati, OH 45202

JOHN H. ZACHARIA
NATHAN P. JUDISH
U.S. Department of Justice
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20005

STEVEN L. LANE
U.S. Department of Justice
950 Pennsylvania Ave., N.W., Rm. 1264
Washington, D.C. 20530

MARTIN G. WEINBERG, ESQ.
20 Park Plaza, Suite 905
Boston, MA 02116

MARTIN S. PINALES, ESQ.
105 W. 4th St., Suite 920
Cincinnati, OH 45202

KEVIN S. BANKSTON
Electronic Frontier Foundation
454 Shotwell St.
San Francisco, CA 94110

ORIN S. KERR
Professor of Law
George Washington University Law School
2000 H Street, N.W.
Washington, D.C. 20052

_____

PATRICIA L. BELLIA
Notre Dame Law School
Notre Dame, IN 46556
(574) 631-3866