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

Appeal from the United States District Court
For the Southern District of Ohio

BRIEF OF AMICUS CURIAE ORIN S. KERR IN FAVOR OF THE PETITION OF THE UNITED STATES FOR REHEARING EN BANC

ORIN S. KERR
Professor, George Washington
University Law School
2000 H Street, NW
Washington DC 20052
(202) 994-4775
(affiliation for identification purposes
only)

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

STATEMENT OF INTEREST

Amicus is a law professor who teaches and writes in the area of computer crime law. His publications include a casebook on computer crime law and several law review articles on how the Fourth Amendment should apply to computers and new technologies. Amicus believes that this case raises critically important questions of first impression concerning how the Fourth Amendment applies to the Internet. He has written this brief to help the Court understand the significance of this case. He has no interest in the outcome of this litigation except as it relates to these concerns.

SUMMARY OF ARGUMENT

The petition for rehearing en banc should be granted. The panel decision in this case is an extraordinary departure from established precedent with profound implications for the future of constitutional criminal procedure. In one decision, with essentially no facts before the court, the panel conjured up a comprehensive constitutional regime for e-mail privacy in a way counter to well-established limits on the judicial power. The panel's new regime effectively rewrote the law of e-mail privacy from scratch, invalidating one federal statute and shedding serious constitutional doubt on several others.

If permitted to stand, the panel opinion will be a highly troubling precedent. The Fourth Amendment has traditionally developed case-by-case in a gradual process based on particular facts. The panel ignored this tradition. It interpreted a motion for injunctive relief as an invitation to identify all of the hypothetical cases in which the Fourth Amendment could possibly be violated. Under the guise of tailoring an injunction to Constitutional needs, the panel embarked on a free-ranging inquiry that created an entirely new regime of constitutional law.

The Supreme Court has rejected this all-at-once approach, making the panel's endorsement of this procedure quite remarkable. If allowed to stand, the panel's approach will have dramatic implications for how Fourth Amendment rules are made. It will encourage courts to craft Fourth Amendment rules through the scope of injunctions far removed from actual cases and controversies. In light of the extraordinary nature of the panel decision, the petition for rehearing should be granted. The full Court needs to hear this case.

ARGUMENT

I. THE PANEL DECISION IS A BREATHTAKING DEPARTURE FROM HOW FOURTH AMENDMENT RULES ARE CREATED AND HAS DRAMATIC IMPLICATIONS FOR THE FIELD OF CONSTITUTIONAL CRIMINAL PROCEDURE

Fourth Amendment law traditionally develops in a case-by-case fashion. *Saucier v. Katz*, 533 U.S. 194, 205-06 (2001); *United States v. Brown*, 635 F.2d 1207, 1211 (6th Cir. 1980). Every decision is based on concrete facts. *See v. City of Seattle*, 387 U.S. 541, 546 (1967). After a search or seizure occurs, the subject files a civil action or a motion to suppress. The trial court holds a hearing if necessary and applies the Fourth Amendment to the facts established in the record. *See, e.g., Michigan Dept. of State Police v. Sitz*, 496 U.S. 444, 448-49 (1990) (noting the "extensive testimony" heard to determine the constitutionality of a highway checkpoint program).

Injunctive relief is rare in Fourth Amendment cases. Courts only grant injunctive relief when the government has an ongoing program such as a drug testing policy or a road block program. In such cases, courts determine the facts of the ongoing program and decide whether the program as it exists is constitutional or unconstitutional. *See, e.g.*, *Sitz*, 496 U.S. at

448-49; *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000); *National Treasury Employees Union v. Von Raab*, 489 U.S. 655 (1989). Courts do not engage in a hypothetical examination of what other conceivable programs might or might not be legal. They stick to the facts in the record.

This case-by-case approach is crucial to the overall design of Fourth Amendment rules. The Supreme Court has emphasized this point in its cases discouraging "facial" Fourth Amendment challenges to statutes. When a court permits a facial challenge, it considers the range of possible practices authorized under a statute rather than the specific facts before the Court. Although the Supreme Court permitted a Fourth Amendment facial challenge once, in the unusual circumstances of *Berger v. New York*, 388 U.S. 41 (1967),[1] the Court dramatically narrowed the meaning of *Berger* just months later in *Sibron v. New York*, 392 U.S. 40 (1968). In *Sibron*, Chief Justice Warren explained that it was improper to subject a statute to facial Fourth Amendment challenge outside the specific context of a statute authorizing the issuance of search warrants: "The constitutional validity of a warrantless search is pre-eminently the sort of question which can only be

[1] *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 847-49 (2004).

decided in the concrete factual context of the individual case." *Id*. at 59. Thus the question in the usual case was not whether the statute was constitutional but whether the searches and seizures conducted pursuant to the statute were constitutional. *Id*. at 59-62.

The Supreme Court has only become more skeptical of facial challenges since *Sibron*. Just recently, in *Sabri v. United States,* 541 U.S. 600 (2004), the Court warned about the dangers of permitting facial challenges outside of a few specific recognized categories: "Although passing on the validity of a law wholesale may be efficient in the abstract, any gain is often offset by losing the lessons taught by the particular, to which common law method normally looks. Facial adjudication carries too much promise of premature interpretation of statutes on the basis of factually barebones records." *Id*. at 608-09. *See also Skinner v. Railway Labor Executive' Ass'n,* 489 U.S. 602, 614-15 (1989) (refusing a program-wide Fourth Amendment challenge to drug and urine tests because the facts of each test may be different).

The panel decision ignored these teachings. It reconfigured the field of e-mail privacy without even a factual hearing. Indeed, the panel did more than allow a facial challenge. It allowed a challenge to *every conceivable set of facts* in which the government compels e-mail from an ISP, regardless of

whether the practice happens to be regulated by the challenged statute or not. Citing *Berger* and ignoring *Sibron* and *Sabri*, the panel envisioned its task as crafting an injunction that would permit only constitutional practices. This allowed the panel to address and resolve the constitutionality of obtaining e-mail in every circumstance imaginable.

The panel opinion is very complicated, and several very important points are made only in passing or without extended discussion. But the panel's new set of rules appears to be the following:

> (a) When the government seeks to compel the contents of personal e-mails from an Internet service provider, it may obtain the e-mail from the Internet service provider only in the following circumstances:
>
> (1) Pursuant to a subpoena, if the government can establish, "based on specific facts," "that the ISP or other intermediary clearly established and utilized the right to inspect, monitor, or audit the contents, or otherwise had content revealed to it," or:
>
> (2) Pursuant to a subpoena, if the government provides prior notice to the e-mail subscriber and permits the subscriber an opportunity to challenge the constitutional reasonableness of the subpoena before the e-mails are disclosed, or:
>
> (3) Pursuant to a search warrant based on probable cause that "target[s] e-mails that could reasonably be believed to have some connection to its specific investigation," if neither the circumstances in subsections (1) or (2) are satisfied.
>
> (b) Subsection (a) shall not apply to computer scanning of e-mail for key words, types of images or "similar indicia of wrongdoing" in a way that does not disclose contents to an actual person.

As a matter of policy, this set of rules has some strengths and some weaknesses. But as the work of a single legal decision, it is astonishing. It creates new answers to a remarkable range of unsettled questions, and in the course of it invalidates much of 18 U.S.C. § 2703, the federal statute that for the last 20 years has regulated efforts to compel e-mail from Internet service providers. It also indicates that Congress's distinction between § 2703(a) and § 2703(b) is constitutionally invalid; that the delayed notice provisions of § 2705 are unlawful as well; and it also sheds considerable constitutional doubt on 18 U.S.C. § 2511(i), a provision of the Wiretap Act known as the "computer trespasser" exception. *See generally* Orin S. Kerr, Computer Crime Law 482-87, 501-07, 516-18 (2006) (discussing these provisions).

The panel should not have reached all of these questions. First, the court has no jurisdiction to entertain a claim for injunctive relief unless Warshak can establish a "real or immediate threat" that the United States will seek his e-mail from an ISP in the future using less process than a warrant. *Williams v. Ellington*, 936 F.2d 881, 888 (6th Cir. 1991). That threat seems remote in the context of this case, suggesting that Warshak's remedies should be limited to pursuing his civil case for damages and seeking suppression of evidence in his criminal case if needed. But even if the court concludes the threat of a future event is real and immediate, and

that injunctive relief is therefore permitted, the scope of injunctive relief should only consider whether the one procedure likely to occur again is constitutional or not.

Nor is this simply an academic point. If permitted to stand, the panel decision will have tremendous practical significance. From a plaintiff's perspective, there are obvious tactical benefits to litigating Fourth Amendment claims in civil cases rather than in the context of a motion to suppress. The panel opinion gives plaintiffs a remarkable new tool for litigating Fourth Amendment claims. Under the panel's approach, plaintiffs can identify a category of law enforcement practice, show that it might be used again against the plaintiff in the future, and then seek an injunction that calls on the court to draft a new constitutional framework that settles all of the ways in which that practice might be used. Today the facts involve e-mail. But what's next? Roadblocks? Drug tests? Traffic stops? Home searches? If this Court wants to empower the judiciary to resolve broad swaths of Fourth Amendment law all at once in this manner, its decision allowing such procedures should come from the full Court rather than a three-judge panel.

II. THE EXTRAORDINARY RANGE OF NOVEL AND IMPORTANT FOURTH AMENDMENT QUESTIONS ADDRESSED IN THE PANEL OPINION INCLUDES SEVERAL CONCLUSIONS THAT ARE HIGHLY QUESTIONABLE OR SIMPLY WRONG.

The Supreme Court's insistence on case-by-case decisionmaking has been motivated by the need for accuracy. *Sabri v. United States*, 541 U.S. 600, 608-09 (2004). It rests on the insight that "[a] more evolutionary approach, involving the accretion of case-by-case judgments, could produce fewer mistakes on balance, because each decision would be appropriately informed by an understanding of particular facts." *Name.Space, Inc. v. Network Solutions, Inc.*, 202 F.3d 573, 584 n. 11 (2d Cir. 2000).

Unfortunately, the panel's many dramatic conclusions about cutting-edge questions of Fourth Amendment law showcase the dangers of the contrary "all at once" approach. No single set of legal briefs can adequately articulate the competing arguments behind the dozen or so novel questions of law the panel attempted to answer. As a result, while some of the panel's conclusions are quite plausible, others are a serious stretch and a few appear to be simply wrong.

A full accounting of the panel's errors and questionable moves is beyond the scope of this short brief.[2] However, a few obvious difficulties are worth noting here. First, the panel's framework depends heavily on the distinction between expectations of privacy vis-a-vis ISPs and expectations of privacy vis-a-vis the public. *See* Slip. Op. at 9. No such distinction exists. The Fourth Amendment only recognizes one kind of constitutionally reasonable expectation of privacy, and a defendant either has one or he does not. If a party has rights against the public but not rights against a provider, that should be a question of third-party consent rather than reasonable expectations of privacy.

Second, the panel concludes that even if a defendant has a reasonable expectation of privacy in his e-mail, prior notice would allow the government to subpoena the e-mail under a low reasonableness standard rather than probable cause. That is, the panel envisions a tradeoff: the Constitution demands either probable cause or notice but not both. See Slip. Op. at 9. This is a completely novel idea, however, and the panel cites no relevant authority for it. The panel opinion repeatedly invokes *United States*

---

[2] For a partial discussion, see the links from Orin S. Kerr, *A Series of Posts on Warshak v. United States, the E-Mail Privacy Case*, The Volokh Conspiracy, available at http://www.volokh.com/posts/1182208168.shtml.

v. Phibbs, 999 F.3d 1053 (6th Cir. 1993), but the undersigned has been unable to understand how *Phibbs* relates to the role of notice in setting the constitutional standard for a subpoena.

Finally, the panel's statements about the rights of computer hackers and those with expired e-mail accounts are at sharp odds with the Supreme Court's most relevant precedents. The panel suggests that a person has Fourth Amendment rights in e-mail if there are good chances that no one else would look at his e-mail. Because a hacker or a person with an expired account wouldn't expect others to look at his e-mail, he retains Fourth Amendment rights in his account. *See* Slip. Op. at 17. This theory is plainly inconsistent with the Supreme Court's most analogous decisions on the Fourth Amendment rights of lessees. Precedents such as *Minnesota v. Carter*, 525 U.S. 83 (1998), and *Minnesota v. Olson*, 495 U.S. 91 (1990), stress that whether a lessee or guest has a reasonable expectation of privacy depends on whether that person has a legitimate and substantial connection to that particular place. Under *Olson*, an overnight guest has Fourth Amendment rights in the home; under *Carter*, a person who visits the home just to bag cocaine does not. The chances that others will enter the space are irrelevant. *See Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) ("A burglar plying his trade in a summer cabin during the off season may have a

thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as 'legitimate.'").

CONCLUSION

How the Fourth Amendment applies to e-mail is one of the most important and difficult questions that courts will face in response to the new problem of computer-related crimes. The questions are too difficult for an all-at-once answer. The rules must be announced case-by-case, step-by-step, in a cautious and careful manner fully informed by the facts. The panel decision's rejection of these principles warrants review by the full Court. The petition of the United States should be granted.

Respectfully submitted,

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

CERTIFICATE OF SERVICE

I certify that I have this day served this brief of Amicus Curiae Orin S. Kerr by causing a true and correct copy thereof to be dispatched by courier or Federal Express, designated for delivery on the same or the next business day, to each of the following addresses:

Steven L. Lane
United States Department of Justice
950 Pennsylvania Ave. NW, Rm. 1264
Washington DC 20530
(202) 514-3740

Martin G .Weinberg
20 Park Plaza, Suite 905
Boston, MA 02116
(617) 227-3700

Martin S. Pinales
105 W. 5th Street, Suite 920
Cincinnati, OH 45202
(513) 721-4876

Kevin S. Bankston
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 631-3866

(continued on the next page)

Patricia L. Bellia
Notre Dame Law School
P.O. Box 780
Notre Dame, IN 46556
(576) 631-3866

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

Dated: August 9, 2007

_____
Orin S. Kerr