No. 09-11897-G

IN THE
UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

CHARLES A. REHBERG,
Plaintiff-Appellee

v.

JAMES P. PAULK et al.,
Defendants-Appellants

APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE MIDDLE DISTRICT OF GEORGIA

BRIEF OF *AMICI CURIAE* LAW PROFESSORS AND INSTRUCTORS SUPPORTING APPELLEE'S PETITION FOR REHEARING OR HEARING EN BANC

Paul Ohm (*pro hac vice*)
California Bar No. 205374
University of Colorado Law School
Samuelson-Glushko Technology
Law & Policy Clinic
401 UCB
Boulder, CO 80309
(303) 492-0384
(303) 492-1200–facsimile

Ralph Scoccimaro
Georgia Bar No. 631525
Brown & Scoccimaro, P.C.
1801 Gillionville Road
Albany Georgia 31701
(229) 432-9310
(229) 436-6302—facsimile

Attorneys for *Amici Curiae*

STATEMENT OF THE ISSUES MERITING EN BANC CONSIDERATION

The panel ruled that individuals have no reasonable expectation of privacy in the contents of stored e-mail messages. This departs significantly from other rulings, contradicts Supreme Court precedent, and jeopardizes millions of e-mail users' privacy. *En banc* consideration is merited for these reasons.

ADOPTION OF STATEMENT OF FACTS NECESSARY TO ARGUMENT OF THE ISSUES

Amici adopt the "Statement of Facts Necessary to Argument of the Issues" offered in Appellee's petition.

ARGUMENT AND AUTHORITIES

A group of law professors and instructors submit this brief *amici curiae* in support of Appellee Charles Rehberg. *Amici* urge this Court to rehear, as a panel or *en banc*, the opinion filed March 11, 2010, *Rehberg v. Paulk*, 2010 WL 816832 (11th Cir. March 11, 2010), and to affirm the District Court's order denying qualified and absolute immunity to Appellants on the basis of the pleadings alone.

The Court's opinion strips all e-mail messages of Fourth Amendment protection: Law enforcement officers can now scrutinize the stored, private e-mail of any person, unrestricted by the Constitution. The police, for example, may now manufacture facially invalid process—as the complaint alleges former District Attorney Hodges did here—compelling e-mail providers to turn over customers' personal, private communications without running afoul of the Fourth Amendment.

The impact of the Court's ruling is hard to exaggerate. Millions of Americans use e-mail every day for practically every type of personal activity and for myriad private uses: to send and receive family photos, personal advice, love letters, personal financial documents, trade secrets, and legally privileged communications. People trust this medium for sensitive, private communication because they expect personal e-mails sent and received over the Internet to be like other forms of personal communication such as sealed letters, telephone calls, or papers stored in a home. Yet the panel's ruling announces that, contrary to these settled expectations, e-mail users have been using a twenty-first century version of a postcard, with no constitutional protection from arbitrary government intrusion.

This is not the first time a court has had to correct such a mistake. In 1928 the Supreme Court held that the Fourth Amendment did not protect the privacy of telephone calls. *See Olmstead v. United States,* 277 U.S. 438, 464-65 (1928) (wiretapping telephone lines outside of bootlegging suspect's home and offices not a search or seizure because no entry made into the properties). In 1967, the Supreme Court recognized *Olmstead* to have been an error that had left telephone users Constitutionally unprotected for nearly half a century. *Berger v. New York*, 388 U.S. 41 (1967) (electronic eavesdropping statute facially unconstitutional for lack of adequate Fourth Amendment safeguards); *Katz v. United States*, 389 U.S. 347 (1967) (finding a Fourth Amendment expectation of privacy in telephone calls

made from a closed phone booth).

This Court should reconsider its ruling to avoid the mistake of *Olmstead* and follow the lessons of *Berger* and *Katz*. *Amici* submit this brief in support of Mr. Rehberg, and millions of other e-mail users, to explain why the Fourth Amendment protects widespread, reasonable expectations of privacy in stored e-mail.

I. E-MAIL USERS POSSESS A REASONABLE EXPECTATION OF PRIVACY IN THE CONTENTS OF THEIR STORED E-MAIL SIMILAR TO THE EXPECTATION OF PRIVACY IN THE CONTENTS OF TELEPHONE CALLS, SEALED LETTERS, AND PRIVATE PAPERS AND EFFECTS.

E-mail users have a constitutionally protected "reasonable expectation of privacy" in their stored e-mail messages under *Katz*. *See id.*, 389 U.S. at 360-61 (Harlan, J., concurring). Fourth Amendment protections apply where "a person [has] exhibited an actual (subjective) expectation of privacy . . . that society is prepared to recognize as [objectively] 'reasonable.'" *Id.* Our reasonable expectation of privacy in stored e-mails is analogous to that in phone calls, sealed postal mail, and private papers and effects.

A. E-mail, like the telephone, plays a vital role in private communication reflecting users' privacy expectations.

The Supreme Court in *Katz* rejected *Olmstead*'s rigid property-based

conception of the Fourth Amendment, holding instead that "the Fourth Amendment protects, people, not places." *Id.* at 351. Even though Mr. Katz's telephone conversations were intangible and not "houses, papers, [or] effects," and even though they were transmitted via the telephone company's property, they were nevertheless protected by the Fourth Amendment against search or seizure. *Compare id. with Olmstead,* 277 U.S. at 465. Mr. Rehberg's stored e-mail messages, and those of the typical e-mail account holder, are no different.

Katz recognized that the Fourth Amendment protects society's shared expectations about what is private and refused "to ignore the vital role that the public telephone has come to play in private communication." *Id.* at 352.

Since *Katz*, the Supreme Court has looked regularly to societal expectations to elaborate the Fourth Amendment, particularly when scrutinizing new technologies. *See Georgia v. Randolph*, 547 U.S. 103, 111 (2006) (search based on spouse's consent over target's objection unreasonable based on "widely shared social expectations" and "commonly held understanding[s]"); *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (technological advances must not be allowed to erode society's expectation in "that degree of privacy against government that existed when the Fourth Amendment was adopted.").

Based on society's extensive use of e-mail for private, sensitive communications, it is plain that society expects and relies on the communication in

this medium to be private, just as with telephone communication. So too with society's expections for *stored* e-mail messages: e-mail users often store many of their personal messages online after they have been sent or received, rather than downloading them onto their own computers.[1] Indeed, the largest e-mail services are successful because they offer users huge amounts of electronic space to warehouse e-mails for perpetual storage.[2] Given these societal patterns, to hold that the millions who store their e-mail with providers such as Google, Microsoft, or Yahoo lack either a subjective or objective expectation of privacy makes no sense, and violates *Katz* by failing to defer to society's expectations of privacy.

B. Stored e-mail is communications content protected by the Fourth Amendment like the content of telephone calls, sealed letters, and personal papers and effects.

In justifying its conclusion that the *content* of stored e-mail deserves no

---

[1] Many e-mail users lack the option of storing e-mail on their own computers. For example, users of Yahoo!'s web-based e-mail service can view e-mail on the service's web site, but cannot download e-mail to their computers. *See* Yahoo!, *Yahoo! Mail Help: Organizing and Accessing E-mail*, *available at* http://help.yahoo.com/l/us/yahoo/mail/original/manage/ (visited Mar. 30, 2010).

[2] Google's "Gmail" service, for example, offers more than seven gigabytes of free storage space. Google, *Google Storage*, *available at* http://mail.google.com/support/bin/answer.py?hl=en&answer=39567 (visited Mar. 30, 2010). Google encourages users not to throw messages away. Google, *Getting Started with Gmail*, *available at* http://mail.google.com/mail/help/intl/en/start.html (visited Mar. 30, 2010) ("Don't waste time deleting . . . . [T]he typical user can go years without deleting a single message.").

Fourth Amendment protection, the panel relied, in part, on the Supreme Court's decisions in *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976). These cases do not support this conclusion but rather stand for the opposite conclusion; *Smith* and *Miller* draw a line between constitutionally-unprotected information voluntarily conveyed to third parties for use by the third parties and constitutionally-protected contents of communications.

The *Smith* court distinguished the contents of phone calls, which it reaffirmed are protected by the Fourth Amendment under *Katz*, from the dialed phone numbers acquired by "pen register" surveillance, which it held are not protected. 442 U.S. at 741-42.[3] *Smith* concluded that dialed phone numbers are not protected by the Fourth Amendment because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," as that person has "assumed the risk" that the information "revealed" to the third party will be conveyed to the government. *Id.* at 743-744. Although the electrical impulses constituting the contents of a telephone conversation are just as exposed

---

[3] Some scholars, including several of the *amici,* have criticized the reasoning in *Smith* and *Miller* and urged courts to apply different rules to modern communications. *E.g.,* Susan Freiwald, *First Principles of Communications Privacy*, 2007 Stan. Tech. L. Rev. 3, ¶¶ 46-49; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1137-38. Here, however, *amici* argue that even assuming the direct applicability of these cases to modern communications, the contents of stored e-mail messages enjoy full Fourth Amendment protection.

to telephone company equipment as dialed numbers, *Smith* made clear that its holding did not disturb *Katz*'s reasoning because "pen registers do not acquire the *contents* of communications." *Id.* at 741 (emphasis in original); *accord United States v. Thompson*, 936 F.2d 1249, 1252 (11th Cir. 1991) (noting that "a device which *merely* records the numbers dialed from a particular telephone line" does not violate the Fourth Amendment) (emphasis added).

Smith thus confirms that spying on what callers say is more invasive than knowing what phone numbers they dial. 442 U.S. at 741 (pen registers "disclose *only* the telephone numbers that have been dialed . . . [not] the purport of any communication between the caller and the recipient.") (emphasis added) (quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977)). This Court has embraced this reasoning; a mere two days before the panel issued the *Rehberg* opinion, another, similarly-composed panel relied on the distinction between the contents of communications and information we voluntarily disclose to providers. *United States v. Beckett*, No. 09-10579, 2010 WL 776049, at *4 (11th Cir. March 9, 2010) ("Beckett could not have had a reasonable expectation of privacy in the information that was obtained from the ISPs and the phone companies. The investigators did not recover any information related to content.") (unpublished *per curiam* opinion by Judges Hull, Wilson, and Anderson).

Moreover, the content of stored e-mail—like the phone call content

protected under *Katz* and *Smith*—is in no way analogous to the business records in *Miller*, but is instead like the contents of the home or one's private papers and effects. As the *Miller* court explained, distinguishing *Katz*, "the documents subpoenaed [were] not respondent's 'private papers'" nor his "confidential communications." *Miller*, 425 U.S. at 440, 442. "Instead, these [were] the business records of the banks," which "pertain[ed] to transactions to which the bank was itself a party," *id.* at 440, and contained only information "exposed to [the bank's] employees in the ordinary course of business." *Id.* at 442.

In contrast, the eavesdropping in *Katz* constituted a search and seizure of intangible conversations, which were constitutionally akin to tangible papers and effects. *See Katz*, 389 U.S. at 352-53 (finding that "[t]he Government's activities in electronically listening to and recording the petitioner's *words* violated the privacy upon which he justifiably relied.") (emphasis added). The Supreme Court has repeatedly reaffirmed that conversations are not mere business records but constitutionally like papers and effects. *See Berger*, 388 U.S. at 51 (holding conversations protected by the Fourth Amendment); *id.* at 63 (treating conversations akin to "the innermost secrets of one's home or office"); *Smith*, 442 U.S. at 741-42 (finding no search or seizure because surveillance devices at issue did not disclose "*the purport of any communication* between the caller and the recipient.") (emphasis added) (quoting *New York Tel. Co.*, 434 U.S. at 167 (1977));

United States v. U.S. District Court, 407 U.S. 297, 313 (1972) ("[T]he broad and unsuspected governmental incursions into *conversational privacy* which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.") (emphasis added). Thus the Fourth Amendment protects *the content of private conversations*, whether tangible or intangible, and regardless of the technology by which those conversations are transmitted.

Many other constitutional analogies apply as well: The Supreme Court has recognized expectations of privacy in the contents of sealed packages and letters. *Ex Parte Jackson*, 96 U.S. 727, 733 (1878). Bank customers expect privacy in the contents of their safe deposit boxes. *United States v. Thomas*, No. 88-6341, 1989 WL 72926, at *2 (6th Cir. July 5, 1989). Tenants in rented residences and hotel rooms maintain Fourth Amendment privacy in their units while they occupy them. *Stoner v. California*, 376 U.S. 483, 489 (1964). Users expect their stored e-mail messages to be treated as privately as any of the above, as evidenced by the sensitivity of the messages they send and amount of information they store.

In the Internet age, many of our most important private conversations have migrated from the telephone and sealed envelope to the e-mail server, and we see no principled reason to depart from the Supreme Court's repeated holdings about conversational privacy. *Katz* and *Smith* require that this Court afford stored e-mail the same protection as papers and effects stored in a person's home.

C. The panel's ruling contradicts the great weight of authority.

Not only did the panel disregard the lessons of *Smith* and *Katz*, but also it went against the great weight of authority, breaking with a long line of courts and scholars who have all concluded that the Fourth Amendment protects the reasonable expectation of privacy users have in stored e-mail messages. Two federal, military appellate courts have afforded Fourth Amendment protection to e-mail. *See, e.g.*, *United States v. Maxwell*, 45 M.J. 406, 418-19 (C.A.A.F. 1996); *United States v. Long*, 64 M.J. 57, 65 (C.A.A.F. 2006). Many Article III courts have come to similar conclusions. *See, e.g., Wilson v. Moreau*, 440 F.Supp.2d 81, 108 (D.R.I. 2006) (finding "a reasonable expectation of privacy in [a user's] personal Yahoo e-mail account"); *In re Applic. of U.S. for Orders Authorizing the Use of Pen Registers*, 515 F. Supp. 2d 325, 336 (E.D.N.Y. 2005) (holding that telephone numbers dialed *after* a call has been initiated—such as account numbers sent to a bank or the commands sent to a voicemail system—are protected contents under *Katz*).

No court before has applied the assumption of risk rationale of *Miller* to e-mail. As one put it,

> The "assumption of risk" . . . is far from absolute. "Otherwise phone conversations would never be protected, merely because the telephone company can access them; letters would never be protected, by virtue

> of the Postal Service's ability to access them; the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company's ability to access them." These consequences of an extension of the assumption of risk doctrine are not acceptable under the Fourth Amendment.

Id. at 338 (citations removed).

Courts of Appeal have concurred. Both the Sixth and Ninth Circuits have extended Fourth Amendment protection to the contents of electronic communications, albeit in opinions both now vacated. First, in *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), the Sixth Circuit noted that "like the telephone earlier in our history, e-mail is an ever increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past." *Id.* at 473. It expressly rejected the assumption-of-risk rationale for stored e-mail, finding that "simply because the phone company or the ISP *could* access the content of e-mail and phone calls, the privacy expectation in the content of either is not diminished, because there is a settled expectation that the ISP or the phone company will not do so as a matter of course." *Id.* at 471 (emphasis in original). Importantly, the court explained that its earlier decision in *Guest v. Leis*, which is the principal opinion relied upon by the

panel in *Rehberg*, should not be read to deny constitutional protection to the contents of e-mail messages. *Id.* at 472 ("*Guest* did not hold that the mere use of an intermediary such as an ISP to send and receive e-mails amounted to a waiver of a legitimate expectation of privacy."). Second, and in similar terms, the Ninth Circuit found that users of a text messaging service possessed a Fourth Amendment reasonable expectation of privacy, because it could find "no meaningful distinction between text messages and letters." *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 506 (9th Cir. 2008). Although both of these opinions have now been vacated—*Warshak* as not ripe, 532 F.3d 521, 523 (6th Cir. 2008), *Quon* by the Supreme Court upon its grant of certiorari, 130 S. Ct. 1011 (2009)—each opinion's discussion of our reasonable expectation of privacy of e-mail is persuasive. *Warshak* provides a detailed and careful explanation for why e-mail contents are constitutionally protected, and *Quon* directly applies the Ninth Circuit's earlier reasoning in *United States v. Forrester*, 495 F.3d 1041 (9th Cir. 2007). In *Forrester*, the Ninth Circuit analogized electronic mail to physical mail:

> E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical. The contents may deserve Fourth

> Amendment protection, but the address and size of the package do not.

Id. at 1049

Finally, courts have found expectations of privacy in e-mail outside the Fourth Amendment context. For example, several courts have extended the attorney-client privilege to e-mail messages, finding both subjective and objective expectations of privacy. *See*, *e.g.*, *Stengart v. Loving Care Agency*, 2010 N.J. LEXIS 241, *38-39 (N.J. March 30, 2010) ("Stengart could reasonably expect that e-mails she exchanged with her attorney on her personal, password-protected, web-based e-mail account, accessed on a company laptop, would remain private."); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F.Supp.2d 548, 565 (S.D.N.Y. 2008) (user "had a reasonable subjective and objective belief that his [Hotmail] communications would be kept confidential").

The panel's decision singles out this Court as the only court at any level to rule unequivocally and without limitation that the contents of e-mail messages are completely unprotected by the Fourth Amendment.

The panel's opinion also conflicts with the apparently unanimous opinion of legal scholars. Scholars, including many of the *amici*, have argued at length that users have a reasonable expectation of privacy in the contents of e-mail messages. *E.g.,* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored*

E-Mail, 2008 U. Chi. L. F. 121, 135-140; Deidre Mulligan, *Reasonable Expectations of Privacy in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1591 (2004); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, *at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1348322, at 33 (forthcoming Stan. L. Rev., 2010) (setting out a presumption that the contents of communications are normally protected by the Fourth Amendment); Stephen Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 Mercer L. Rev. 507, 527 (2005) ("[A]s with postal mail and telephone conversations, the sender of e-mail retains no REP in the addressing components, but should retain a REP in the content"). *Amici* know of no scholars who have concluded otherwise.

The panel's ruling is contrary to Supreme Court precedent, other lower-court decisions, and scholarly consensus, and disrupts the settled expectations of millions of e-mail users. This Court should therefore grant Appellee's petition.

II. THE PANEL'S RULING WILL JUSTIFY UNDULY EXPANSIVE NEW POLICE SURVEILLANCE.

If this Court's ruling stands, the privacy of the e-mail users in this Circuit will be placed in sudden jeopardy. Left without the protection of the Fourth Amendment, they will find their privacy protected only by the Stored

Communications Act (SCA), 18 U.S.C. § 2701 *et seq.*, which falls far short of ensuring the level of privacy promised by the Fourth Amendment. As only one example, those harmed by SCA violations have no suppression remedy. 18 U.S.C. § 2708 ("Exclusivity of remedies"). Overzealous law enforcement officials will be free to manufacture sham subpoenas to obtain the e-mails of any person without the disincentive of possible suppression. This is no hypothetical: these are the very facts alleged by Mr. Rehberg and weighed by the district court in concluding the defendants did not deserve qualified or absolute immunity. We urge this Court to rehear this case and affirm the decision of the district court.

CONCLUSION

For these reasons, the Court should grant the petition for a panel rehearing or hearing *en banc* and affirm the District Court's decision.

DATED: May 24, 2010

By _____

Paul Ohm (*pro hac vice*)
University of Colorado Law School
Samuelson-Glushko Technology
Law & Policy Clinic
401 UCB
Boulder, CO 80309
(303) 492-0384
(303) 492-1200–facsimile