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 OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, ACLU OF OHIO FOUNDATION, INC., AMERICAN CIVIL LIBERTIES UNION, AND CENTER FOR DEMOCRACY AND TECHNOLOGY SUPPORTING THE APPELLEE AND URGING AFFIRMANCE

Kevin S. Bankston
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333 x 126
(415) 436-9993 – facsimile

Attorneys for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Law Review Articles and Treatises

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to FRAP 26.1, *amici* Electronic Frontier Foundation ("EFF"), ACLU of Ohio Foundation, Inc. ("ACLU of Ohio"), American Civil Liberties Union, and Center for Democracy and Technology ("CDT"), 501(c)(3) non-profit corporations incorporated in the States of Massachusetts, Ohio, and Washington, D.C. (both ACLU and CDT), respectively, make the following disclosure:

1. No *amicus* is a publicly held corporation or other publicly held entity.

2. *Amici* have no parent corporations.

3. No publicly held corporation or other publicly held entity owns 10% or more of any *amicus*.

4. No *amicus* is a trade association.

November 22, 2006

Kevin S. Bankston
Staff Attorney
Electronic Frontier Foundation

STATEMENT OF AMICI CURIAE

Amici are non-profit public interest organizations seeking to ensure the preservation of Fourth Amendment protections in the face of advancing technology.

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect free speech and privacy rights in the online world. As part of that mission, EFF has served as counsel or amicus in key cases addressing electronic privacy statutes and the Fourth Amendment as applied to the Internet and other new technologies. With more than 10,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to web sites in the world, www.eff.org.

The ACLU of Ohio Foundation, Inc. ("ACLU of Ohio") is devoted to the preservation and advancement of civil liberties for all Ohioans through public education and litigation. The ACLU of Ohio regularly appears in this Court as either direct counsel or amicus to serve those ends. Because of its particular commitment to rights of privacy and due process, the ACLU of Ohio has a special interest in, and expertise to address, the application of the law in this case.

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with over 500,000 members dedicated to

the principles of liberty and equality embodied in the U.S. Constitution. The protection of privacy as guaranteed by the Fourth Amendment is an area of special concern to the ACLU. In this connection, the ACLU has been at the forefront of numerous state and federal cases addressing the right of privacy in Internet communications.

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 and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

Plaintiff-Appellee Steven Warshak and Defendant-Appellant United States of America have consented to the filing of this amicus brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

EFF, joined by ACLU of Ohio, ACLU, and CDT, respectfully submits this brief *amicus curiae* in support of Appellee Steven Warshak. *Amici* urge this court to affirm the District Court's order preliminarily enjoining the government from seizing the contents of personal email stored by an Internet Service Provider ("stored email") without prior notice to the email account holder. R.21, Order granting in part and denying in part Motion for TRO ("Order"). *Amici* agree with the District Court that 18 U.S.C. §§ 2703(b)(1)(B)(ii), 2703(d) and 2705 facially violate the Fourth Amendment to the extent they allow the search and seizure of stored email contents without notice or a probable cause warrant.[1] Order at 18.

This case must be considered in the context of one overriding fact: millions of Americans use email every day for practically every type of personal business. Private messages and conversations that once would have been communicated via postal mail or telephone now occur through email, the most popular mode of Internet communication.[2] Love letters, family photos, requests for (and offerings of) personal advice, personal financial documents, trade secrets, privileged legal and medical information—all are

---

[1] *Amici* do not address the statutes' constitutionality as applied in this case, nor the constitutionality of court orders and subpoenas for stored email that are accompanied by prior notice to the email account holder.

[2] *See, e.g.*, Pew Internet & American Life Project, *Generations Online* at 1, *available at* http://www.pewinternet.org/pdfs/PIP_Generations_Memo.pdf (Dec. 2005) (explaining that 90% of all Internet users communicate via email, and describing email as "the most popular online activity.")

exchanged over email, and often stored with email providers after they are sent or received.

These myriad private uses of email demonstrate society's expectation that the personal emails sent and received over the Internet and stored with email providers are as private as a sealed letter, a telephone call, or even papers that are kept in the home. Yet the government asks the Court to announce to email users in this Circuit that, contrary to their expectations, they have actually been sending and storing "e-postcards" instead of email all along, and that the Fourth Amendment does not protect their messages against government intrusion. *See* Order at 8-10 (rejecting government's analogy of email to postcards).

The U.S. Court of Appeals for the Armed Forces has already twice ruled that email account holders have a reasonable expectation of privacy in their stored email. *See United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006); *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996). However, this Court is the first Article III appellate court charged with applying long-overdue scrutiny to that question, and to the constitutionality of the federal Stored Communications Act ("SCA"),[3] which in some cases allows the government to obtain email content stored by an Internet Service Provider ("ISP" or

---

[3] This is the common name for the portion of the Electronic Communications Privacy Act ("ECPA") that regulates stored communications and records. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, sec. 201, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C. §§ 2701 *et seq*.).

"email provider") without a probable cause warrant and without prior notice to the email account holder. The Court now faces this question as a result of Steven Warshak's suit to stop the government's repeated, secret searches and seizures of his stored email using court orders authorized under 18 U.S.C. § 2703(d) of the SCA.

In 1928, Faced with a similar choice regarding the Fourth Amendment's application to a new communications technology—the telephone—and over Justice Brandeis' famously prescient objections, the Supreme Court took the wrong path and 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) (government's wiretapping of telephone lines outside of bootlegging suspect's home and offices was not a search or seizure because there was no entry into the suspect's properties). This mistake was not corrected until 1967, leaving the Fourth Amendment rights of telephone users unprotected for nearly half a century. *See Berger v. New York*, 388 U.S. 41 (1967) (finding state's 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, which was violated when the government installed a listening device on the outside of the booth).

This Court should avoid the mistake of *Olmstead* and instead follow the lessons of *Berger* and *Katz*. *Amici* submit this brief in support of Mr.

Warshak and all the other millions of email account holders whose privacy is at stake to argue that: (I) email users possess a reasonable expectation of privacy in their stored email that is protected by the Fourth Amendment; (II) the Fourth Amendment requires, at the very least, a probable cause warrant or prior notice to the email account holder before the government may search or seize stored email; and (III) the SCA is facially unconstitutional to the extent it allows otherwise.

ARGUMENT

I. EMAIL USERS HAVE A REASONABLE EXPECTATION OF PRIVACY IN THEIR STORED EMAIL.

Under the reasoning of *Katz*, the keystone of modern Fourth Amendment doctrine, email users have a constitutionally protected "reasonable expectation of privacy" in their stored email. *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.'"). The reasonableness of such an expectation of privacy in the contents of stored emails is made plain by analogy to society's expectations of privacy in the contents of phone calls, the contents of rental residences like apartments and hotel rooms, and the contents of sealed postal mail.[4] The privacy protections

[4] *Amici* do not address the analogy of stored email to postal mail and other sealed containers, which is fully addressed by Appellee Warshak, *see* Proof Brief of Plaintiff-Appellee Steven Warshak ("Warshak Brief") at 29-31, and other *amici, see* Brief for Professors of Electronic Privacy Law and Internet

of the Stored Communications Act, as well as the privacy policies of email providers, provide further support for the objectively reasonable expectation that stored email is private.

A. Email users possess a reasonable expectation of privacy in the contents of their stored email that is analogous to the expectation of privacy in the contents of telephone calls.

1. Email, like the telephone, plays a vital role in private communication that reflects users' reasonable expectation of privacy.

The Supreme Court in *Katz* rejected *Olmstead*'s strictly property-based conception of the Fourth Amendment, holding instead that "the Fourth Amendment protects, people, not places." *Id.* at 351. Therefore, even though Mr. Katz's telephone conversations were intangible and not literally his "houses, papers, [or] effects," and even though they were transmitted via the phone company's property, they were protected by the Fourth Amendment against search or seizure by the government. *Compare id*. *with Olmstead*, 277 U.S. at 465. Mr. Warshak's emails, and those of the typical email account holder, are no different.

Katz recognized that the Fourth Amendment protects society's shared expectations about what is private, and applied Fourth Amendment protections based on the telephone's vital societal role as a medium for private communication. *Id.* at 352 ("To read the Constitution more narrowly

---

Law as *Amici Curiae* Supporting the Appellee ("Law Professors' Brief") at 13; *see also Maxwell*, 45 M.J. at 417-418 (analogizing stored email to postal mail).

is to ignore the vital role that the public telephone has come to play in private communication."). Society's reliance on public telephones for private communication evidenced its reasonable expectation that those phone calls were in fact private, establishing Fourth Amendment protection as a general matter. *See id*.

Since *Katz*, the Supreme Court has regularly looked to societal expectations in judging Fourth Amendment problems, particularly where new technologies are concerned. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (recognizing that 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"), *Georgia v. Randolph*, ___ U.S. ___, 126 S.Ct. 1515, 1526 (2006) (finding search based on spouse's consent unreasonable based on "widely shared social expectations" and "commonly held understanding[s]").

Based on society's extensive use of email for private communications, it is plain that society expects and relies on the privacy of messages that are sent or received using email providers just as it relies on the privacy of the telephone system. It is equally plain that society expects privacy in stored email: email users often store many if not all of their personal messages with the provider after they have been sent or received, rather than downloading them onto their own computers.[5] Indeed, the largest email services are

[5] Many email users don't even have the option of storing their emails on their own computers. For example, users of Yahoo!'s free web-based email

popular precisely because they offer users huge amounts of computer memory to warehouse their emails for perpetual storage.[6] In light of these facts, to hold that the hundreds of millions of people who store their email messages with Google or Microsoft or Yahoo! have knowingly exposed their emails to the public and voluntarily assumed the risk that those messages will be broadcast to the world makes no sense, and would plainly violate *Katz* by failing to defer to society's expectations of privacy.

2. Stored email, like a telephone call, is communications content protected by the Fourth Amendment.

The Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), reaffirms that the Fourth Amendment protects the contents of stored email messages just as it protects the contents of phone calls.

(webmail) service can only view their email on the service's web site, and cannot download their email messages into an email program on their own computers. *See* Yahoo!, *Yahoo! Mail Help: Client vs. Web-Based Email*, *available at* http://help.yahoo.com/help/us/mail/pop/pop-35.html (last visited Nov. 21, 2006). Yahoo!'s webmail service is the second most popular, with 220 million users. *See* Digital Home Magazine, *Webmail Wars: Hotmail v Yahoo v Gmail*, *available at* http://blog.digitalhomemag.com/page/digitalhome?entry=who_wins_the_battle_of (Nov. 17, 2006).

[6] For example, Google's "Gmail" webmail service currently offers over two gigabytes of storage space, and encourages its users not to throw messages away. Google, *Getting Started With Gmail*, *available at* http://www.google.com/mail/help/start.html (last visited Nov. 21, 2006) ("Don't waste time deleting messages…. [T]he typical user can go years without deleting a single message."). One gigabyte, according to Google, is equivalent to *500,000 pages* of email text. Google Press Release, *Google Gets the Message, Launches Gmail*, *available at* http://www.google.com/press/pressrel/gmail.html (Apr. 1, 2004).

The *Smith* court strongly 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 found are not protected. *Id.* at 741-42.[7] *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, *citing, inter alia*, *United States v. Miller*, 425 U.S. 435, 442-44 (1976) (holding that bank customer had no reasonable expectation of privacy in checks, financial statements, and deposit slips held by bank). However, and despite the fact that the electrical impulses constituting a telephone conversation are as exposed 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). In sum, *Smith* held that *Miller*'s assumption-of-risk analysis does not apply to communications content.

The constitutional import of the "content" concept introduced in *Smith* is twofold. First and most simply, it bears on the invasiveness of the search:

---

[7] *Amici* do not acknowledge that *Smith* was correct in holding that dialed phone numbers are not protected by the Fourth Amendment, but instead cite it only for the holding that the contents of communications *are* so protected.

spying on what callers are saying is more invasive than knowing what phone numbers they are dialing. *See id., quoting United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977) (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)).

Second and more importantly, *Smith*'s treatment of content clarifies *Katz*'s recognition that even though phone conversations are carried by and exposed to phone company equipment, callers have a Fourth Amendment-protected interest in the content of those communications that is directly analogous to the interest in their actual houses, papers and effects. *Olmstead* had held that the Fourth Amendment "can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office," which "are not part of his house or office any more than are the highways along which they are stretched." *Olmstead*, 277 U.S. at 465. The Supreme Court in *Katz* and *Smith* firmly rejected that technology-based distinction.

The content of stored email—like the phone call content protected under *Katz* and *Smith*—is in no way analogous to the business records at issue in *Miller*, but is instead analogous to the contents of the home, or one's private papers and effects. As the *Miller* court explained when distinguishing *Katz*, "the documents subpoenaed are not respondent's 'private papers'" nor his "confidential communications," and "respondent can assert neither ownership nor possession. Instead, these are *the business records of the*

banks," which "pertain to transactions to which the bank was itself a party" and contain only "information exposed to [the bank's] employees in the ordinary course of business." *Miller*, 425 U.S. at 442 (emphasis added).

In contrast, the eavesdropping in *Katz* constituted a search and seizure of *Katz's conversations*, which although intangible were constitutionally akin to his own tangible papers and effects. *See Katz*, 389 U.S. at 352-53 (characterizing government's electronic eavesdropping on conversations as a "search and seizure" of those conversations under the Fourth Amendment, and 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); *see also Berger*, 388 U.S. at 51, 63 ("*conversation*" protected by the Fourth Amendment and akin to "the innermost secrets of one's home or office"); *Smith*, 442 U.S. at 741-42, *quoting New York Tel. Co.*, 434 U.S. at 167 (1977) (finding no search or seizure because the surveillance devices at issue did not disclose "*the purport of any communication* between the caller and the recipient…." (emphasis added)); and *United States v. U.S. District Court*, 407 U.S. 297, 313 (1972) ("the broad and unsuspected governmental incursions into *conversational privacy* which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.") Taken together, these cases clarify *Katz*'s recognition that the Fourth Amendment protects *the content of private conversations*, whether tangible or intangible and regardless of whether those conversations are carried over phone lines—or the Internet.

Both of these aspects of a search or seizure of call content—the high degree of invasiveness and the violation of a Fourth Amendment interest equivalent to that in one's private papers—apply equally to stored email. As already discussed, email users treat their accounts as a storage space, warehousing a broad range of personal communications sent and received over months or even years. And, more than just containing the content of text communications, these emails often contain pictures, video, audio, links to web sites and other resources, and more.[8] Government access to this breadth and depth of communications content is *at least* as invasive as electronic eavesdropping or wiretapping of telephone calls, which only acquires the human voice and only for a relatively short period of time, usually no more than thirty days. *See* 18 U.S.C. § 2518(5). Furthermore, the contents of those messages are plainly analogous to the account holder's own private papers, as opposed to records of the email provider created in the ordinary course of business. Indeed, some popular email providers expressly state in their terms of service that they do not claim ownership of the emails that are stored with them.[9] In light of these facts, *Katz* and *Smith*

---

[8] *See, e.g., Yahoo! Press Release, Yahoo! Mail Announces 1GB of Storage to All Users*, available at http://www.newswiretoday.com/news/548/ (May 6, 2005) ("Yahoo! Mail now offers a whopping 1GB of free email storage. Now keep all those important emails – including ones attached with files, photos, even videos.")

[9] *See, e.g.,* Yahoo!, *Yahoo! Terms of Service*, *available at* http://docs.yahoo.com/info/terms/ (last visited Nov. 21, 2006) ("Yahoo! does

require that this Court afford stored email the same protection as papers and effects stored in a person's home.

3. Email providers' access to stored email content, like telephone companies' access to phone call content, does not diminish their users' constitutional expectation of privacy.

The government places great significance on the fact that email providers have the technical ability to access, and in some cases may access, the email content stored on their computers. However, as *Katz* and *Smith* make clear, this fact is irrelevant to the customer's expectation of privacy in the *contents* of their communications. "A telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment." *Smith*, 442 U.S. at 746 (Stewart, J., dissenting). "Yet," despite telephone providers' potential and actual surveillance of phone calls, the Supreme Court has "squarely held that the user of even a public telephone is entitled 'to assume that the words he utters into the mouthpiece will not be broadcast to the world.'" *Id.* at 746-47, *quoting Katz*, 389 U.S. at 352. Put simply, the potential exposure of telephone call content to a phone company's linesmen and fraud investigators does not eliminate a caller's expectation of privacy against the government.

Phone service subscribers retain this expectation despite the fact that,

---

not claim ownership of Content you submit or make available for inclusion on the Service. . . .").

at common law, they have impliedly consented to eavesdropping by the phone company that is reasonably necessary to effectively maintain the service or prevent its fraudulent use. *See, e.g.*, *Bubis v. United States*, 384 F.2d 643, 648 (9th Cir. 1967), *citing Brandon v. United States*, 382 F.2d 607 (10th Cir. 1967) and cases therein cited. This common law "provider exception" to statutory wiretapping claims existed when *Katz* was decided, and was codified in 1968's federal Wiretap Act and subsequent amendments:

> It shall not be unlawful under this chapter for… a provider of wire or electronic communication service… to intercept, disclose, or use [a] communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service….

18 U.S.C. § 2511(2)(a)(i). Yet no court has ever indicated that such provider access—or a subscriber's implied consent to it—negates the subscriber's expectation of privacy.[10]

---

[10] Notably, the Yahoo! terms of service concerning Yahoo!'s access to its customers' email essentially track the existing provider exception:

> You acknowledge, consent and agree that Yahoo! May access…your…Content…in a good faith belief that such access[,] preservation or disclosure is reasonably necessary to: (a) comply with legal process; (b) enforce the TOS, (c) respond to claims that any Content violates the rights of third parties; (d) respond to your requests for customer service; or (e) protect the rights, property or personal safety of Yahoo!, its users and the public.

Yahoo!, *Yahoo! Terms of Service, available at* http://docs.yahoo.com/info/terms/ (last visited Nov. 21, 2006). Similarly, the NuVox terms of service state "NuVox may access and use individual

Similarly, neither the potential exposure of stored email to an email provider's system administrators in the course of their duties, nor the use of junk-mail and virus filters, eliminates an email user's expectation of privacy. To hold otherwise would pose a constitutional Catch-22 that ignores the vital role that email plays in private communication. Providers attempting to offer absolutely private, constitutionally protected communications solutions by swearing off any access to customers' content would be unable to adequately maintain the security and reliability of their services, while Internet users wishing to take advantage of reliable services free of security-threatening computer viruses and crippling amounts of "spam" messages would be forced to sacrifice their Fourth Amendment rights. Such a result would, contrary to *Kyllo*, allow advances in technology to erode long-standing societal understandings of privacy, *see id.*, 533 U.S. at 34, and contrary to *Katz*, force Internet users to accept that the messages they send may be broadcast to the world, *see id.*, 389 U.S. at 352.

Subscriber information in the operation of the Service and as necessary to protect the Service." NuVox Communications, *Acceptable Uses Policy*, *available at* http://www.nuvox.com/index.php/23 (last visited Nov. 21, 2006). This is exactly the type of limited access by the provider that was and is irrelevant under *Katz*'s reasoning. It is also irrelevant that some providers' counsel happen to draft these provisions more expansively than others. *See* Order at note 17 (noting that Yahoo!'s terms are "somewhat more expansive with respect to disclosure" than NuVox's). Such minor variations in particular contract terms cannot alter society's expectation of privacy in email. *See Smith*, 442 U.S. at 745 (refusing "to make a crazy quilt of the Fourth Amendment" by allowing its protections to be dictated by the "practices of a private corporation").

B. Email users possess a reasonable expectation of privacy in the contents of their stored email that is analogous to the expectation in the contents of rented residences.

A second analogy to an existing expectation of privacy—the expectation of privacy in rented residences such as apartments and hotel rooms—further demonstrates that email users' expectation of privacy in their stored email is undiminished by the email providers' actual or potential access to those emails.

The Supreme Court has long held that the privacy of rented residences is protected by the Fourth Amendment, even though the owner may enter as necessary to protect the property or provide the resident with agreed-upon services. The Supreme Court summarized the settled law in this area in 1964, when considering the search of a hotel room that was authorized by a hotel clerk:

> [W]hen a person engages a hotel room he undoubtedly gives implied or express permission to such persons as maids, janitors or repairmen to enter his room in the performance of their duties. But the conduct of the night clerk and the police in the present case was of an entirely different order. In a closely analogous situation the Court has held that a search by police officers of a house occupied by a tenant invaded the tenant's constitutional right, even though the search was authorized by the owner of the house, who presumably had not only apparent but actual authority to enter the house for some purposes, such as to view waste….
>
> No less than a tenant of a house, or the occupant of a room in a boarding house, a guest in a hotel room is entitled to constitutional protection against unreasonable searches and seizures. That protection would disappear if it were left to depend upon the unfettered discretion of an employee of the hotel. It follows that this search without a warrant was unlawful.

Stoner v. California, 376 U.S. 483, 489 (1964) (internal citations and quotations omitted); *see also Chapman v. United States*, 365 U.S. 610, 616-18 (1961).

The contents of a user's email account, stored on an email provider's computers, are akin to the contents of a hotel room or apartment unit on the property of a hotelier or landlord. Email users store "virtual" papers and effects (emails) in a "virtual" rented home (the email account) that is owned by another (the email provider); the user's password serves as the key to the locked virtual home, assuring its exclusive use. *See Long*, 64 M.J. at 63 (use of password to protect email account contributed to reasonableness of expectation of privacy in stored email).

Furthermore, as in the example of hotel rooms and apartment units, the ability and right of the virtual landlord to enter an email user's virtual home – whether to inspect and maintain the property (i.e., "view waste") or provide agreed-upon services – does not diminish the expectation against invasion by the government, which is of an "entirely different order." *Stoner*, 376 U.S. at 489; see also *Long*, 64 M.J. at 64-65 (distinguishing consent to email monitoring by provider from consent to law enforcement searches).

Put simply, allowing virtual "maids, janitors and repairmen" to enter the virtual home to ensure that it is being properly maintained and cleaned of spam and viruses is of no more account to the Fourth Amendment than a hotel staff's access to a hotel room. *Stoner*, 376 U.S. at 489. To hold

otherwise would violate *Stoner*'s admonition to "bear in mind that it was the [tenant]'s constitutional right which was at stake here…", which "only the [tenant] could waive…." *Id.* As the examples of telephones and rented residences amply demonstrate, email users have not waived their constitutional rights simply by storing their emails with a third-party email provider.

C. The privacy protections in the Stored Communications Act support email users' expectation of privacy in the contents of their stored emails.

Amici do not concede that the SCA necessarily has any relevance to the Fourth Amendment's treatment of stored email, as the government argues. Gov't Brief at 46-48. However, to the extent the statute at all reflects or impacts society's expectation of privacy, it plainly *supports* rather than diminishes the reasonableness of that expectation.

Congress enacted the SCA because it considered communications technologies like email to be analogous to postal mail and telephone calls, and deserving of comparable privacy protection considering society's reliance on them:

> A letter sent by first class mail is afforded a high level of protection against unauthorized opening…. Voice communications transmitted via common carrier are [also strongly] protected…. But there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology. This is so, even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services.

S. REP. NO. 99-541, at 5 (1996). "This gap results in legal uncertainty," which ECPA was intended to address. *Id*.

More than adding new statutory protections, though, ECPA was intended to preserve Fourth Amendment protections for the users of these new technologies. As the Senate explained, in terms echoed by *Kyllo*:

> *Most importantly*, the law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

Id. (emphasis added).

Congress' broad intent to protect the privacy of stored email and preserve Fourth Amendment protections is demonstrated by the fact that it chose to generally require a probable cause warrant for communications contents stored with a communications provider. *See* 18 U.S.C. § 2703(a) ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a[n]… electronic communication… only pursuant to a warrant").

Despite Congress' clear intent to preserve Fourth Amendment protections, the government argues that because the SCA allows for subpoenas and non-warrant court orders in some limited cases, its existence diminishes rather than reinforces any expectation of privacy in email. Gov't Brief at 46-47. However, the two particular arguments it offers on that point are unpersuasive.

First, the government correctly points out that the SCA does not require a probable cause warrant for communications that have been stored for more than 180 days. Gov't Brief at 5-7, 46-47; 18 U.S.C. § 2703(a). However, that provision reflects the state of the technology in 1986, where it was out of the ordinary to store messages for more than ninety days, and it was fair to assume that a six-month old message had probably been abandoned by the user. *See* S. REP. NO. 99-541, at 3 (noting that email providers and other services maintained copies of communications "for approximately 3 months to ensure system integrity"); Deirdre K. Mulligan, *Reasonable Expectations of Privacy in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1569 (2004) (noting that at the time of the SCA's passage, email had to be actively moved into storage to be maintained for more than a few months); and *Maxwell*, 45 M.J. at 412 (at time of trial in 1993, "e-mail [was] stored in AOL's central computer for access and retrieval for 5 weeks to allow for the possibility of vacations and extended trips, and then messages [were] purged from the system.") This now-outdated technical norm has no bearing on how the Fourth Amendment applies to current email services, with their emphasis on remote storage.

Meanwhile, the government's second argument—that Congress intended for stored outgoing emails and opened incoming emails to be obtainable without a warrant, Gov't Brief at 5-6, 46-47—is based on a strained interpretation of the definition of "electronic storage" that lacks any

direct support in the statute's language and has been rejected by the one circuit court to consider it. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2004), *cert. denied*, 543 U.S. 813 (2004) (concluding that opened email is a communication in "electronic storage"); *see also United States v. Councilman*, 418 F.3d 67, 76-77 (1st Cir. 2005) (en banc) (by defining "electronic storage" broadly, "Congress sought to ensure that the messages and by-product files that are left behind after transmission, as well as messages stored in a user's mailbox, are protected from unauthorized access."). Since opened emails are communications in electronic storage, *see Theofel*, 359 F.3d at 1077, the SCA requires the government to obtain a warrant before compelling their disclosure if less than 181 days old. *See* 18 U.S.C. § 2703(a).

Therefore, and taken as a whole, Congress intended the SCA to require a warrant for stored email in most circumstances, and to support rather than diminish email users' constitutional expectation of privacy.

D. Email providers' policies and practices support email users' expectation of privacy in the contents of their stored emails.

Email providers routinely supplement their users' expectation of privacy via official "privacy policies" that delineate the providers' limited authority to access stored email. *See, e.g.*, Yahoo!, *Yahoo! Privacy Policy*, *available at* http://privacy.yahoo.com/ (last visited Nov. 21, 2006) ("Yahoo! takes your privacy seriously…[and] limit[s] access to personal information about you to employees who we believe reasonably need to come into

contact with that information to provide products or services to you or in order to do their jobs."); Google, *Google Privacy Policy*, *available at* http://www.google.com/privacypolicy.html (last visited Nov. 21, 2006) ("At Google we recognize that privacy is important…. Google only processes personal information for the purposes described in the applicable Privacy Policy…."). These representations undermine the government's claim that providers have "unlimited access" to stored email that eliminates constitutional protections, Gov't Brief at 34, and instead only add to the reasonableness of email users' expectation of privacy.

In sum, the government asks this court to disregard society's demonstrated reliance on the privacy of email, a constitutionally-protected expectation supported by statutory protections and privacy assurances made by email providers. The government wrongly suggests that this Court ignore *Katz*'s rejection of a strictly property-based Fourth Amendment, and equate stored email with a *provider's* business records rather than with the content of a *user's* communications. The government makes a similar categorical mistake when arguing that it may search and seize stored email without probable cause.

II. THE FOURTH AMENDMENT REQUIRES A PROBABLE CAUSE WARRANT OR PRIOR NOTICE TO THE EMAIL ACCOUNT HOLDER BEFORE THE GOVERNMENT MAY SEARCH OR SEIZE STORED EMAIL.

The government argues that regardless of an email user's reasonable expectation of privacy, it need only satisfy a "reasonableness" standard to

"compel production" of stored emails from an email provider. Gov't Brief at 36-38. Appellee Warshak and the law professor *amici* have already convincingly debunked this false categorical distinction between compelled production requiring reasonableness and searches and seizures requiring probable cause. *See generally* Warshak Brief at 31-41; Law Professors' Brief at 20-30. However, even assuming that the government's categorical distinction between compelled disclosure and searches or seizures is correct, the government misjudges which category is at issue here, based on a pre-*Katz*, property-focused view of the Fourth Amendment.

Specifically, it is irrelevant whether or not a provider's business records may be subpoenaed under a reasonableness standard, because the stored emails at issue here are not the provider's business records. Rather, they are the account holder's private communications, which he reasonably expects to be as private as his physical papers and effects. Therefore, the compelled disclosure of those communications is a search or seizure requiring prior notice or probable cause. *See People v. Lamb*, 732 P.2d 1216, 1220 (Colo. 1987) (requiring prior notice where subpoena is used to obtain third-party records in which target has reasonable expectation of privacy, in order to avoid unreasonable search or seizure: "the availability of a hearing subsequent to production and disclosure…is inadequate because once the privacy interest has been violated there is no effective way to restore it."); *King v. State*, 535 S.E.2d 492, 497 (Ga. 2000).

From an account holder's perspective, which the Court must bear in

mind is the relevant perspective here, *see Stoner*, 376 U.S. at 489, the government's acquisition of stored email without notice or an opportunity to be heard is simply indistinguishable from a search or seizure under the Fourth Amendment. *See In re Nwamu*, 421 F.Supp. 1361 (S.D.N.Y. 1976), where an FBI agent armed with a grand jury subpoena seized items immediately as if it were a search warrant:

> Taking possession of the items denied movants their right to independent judicial determination of the existence of probable cause as the basis for a search warrant, required by the Fourth Amendment…. The very existence of a right to challenge presupposes an opportunity to make it. That opportunity was circumvented, frustrated and effectively foreclosed by the methods employed here….

Id. at 1365. Here, as in *Nwamu*, an email account holder's standing to seek court review of the government's acquisition of his emails—standing which the government admits exists so long as there is a reasonable expectation of privacy, *see* Gov't Brief at 45, n. 8—presupposes the account holder's ability to seek review *prior to* that acquisition.

The one case that the government cites on the issue of prior notice actually supports its necessity here, and recognizes that government acquisition of private papers held by a third party may violate the target's Fourth Amendment right against unreasonable search and seizure. In *SEC v. Jerry T. O'Brien, Inc.*, the Supreme Court held that because the targets lacked a reasonable expectation of privacy in bank records subpoenaed by the SEC, they were "disable[d]…from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an

unconstitutional search or seizure of his papers." 467 U.S. 735, 743 (1984). Here, by contrast, Amici have demonstrated that email users do have an expectation of privacy in their stored email, which necessitates prior notice so the target may protect against an unconstitutional violation of that expectation. Without such prior notice, that acquisition is necessarily a search and seizure requiring a probable cause warrant.

III. THE STORED COMMUNICATIONS ACT FACIALLY VIOLATES THE FOURTH AMENDMENT TO THE EXTENT IT AUTHORIZES THE SEARCH AND SEIZURE OF STORED EMAIL WITHOUT A PROBABLE CAUSE WARRANT AND ABSENT ADEQUATE PROCEDURAL SAFEGUARDS.

The SCA, like the statute at issue in *Berger*, is facially unconstitutional for its lack of adequate procedural safeguards against unreasonable searches or seizures. *See Berger*, 388 U.S. at 55, 60 ("we have concluded that the statute is deficient on its face," because its "blanket grant of permission to eavesdrop is without adequate judicial supervision or protective measures"). At the very least, the Fourth Amendment requires the government to obtain a probable cause warrant before obtaining stored email without prior notice to the account holder, as that secret acquisition constitutes a search or seizure. The SCA is facially invalid for lacking that single most important Fourth Amendment safeguards, and for failing to include those additional procedural protections that *Berger* found necessary in the context of traditional electronic eavesdropping.

The search and seizure of stored email authorized by the SCA is equally if not more invasive than traditional electronic eavesdropping. Both

modes of surveillance obtain multiple communications of multiple parties made over a period of time, surreptitiously and without particularity. *See Berger*, 388 U.S. at 59 (equating two-month eavesdropping order to "a series of intrusions, searches, and seizures"); *id.* at 60 (insisting on "some showing of special facts" to cure "defect" of not requiring notice); *id.* at 62 (finding that "indiscriminate use of [eavesdropping] devices in law enforcement raises grave constitutional questions") (citation and internal quotation marks omitted).

Yet the SCA is wholly lacking in procedural protections like those that were included in the federal Wiretap Act to avoid the constitutional defects of the statute in *Berger*. Under the Wiretap Act, and consistent with *Berger*:

- Orders authorizing eavesdropping or wiretapping must be based on a judicial finding of probable cause. 18 U.S.C. § 2518(3)(a).
- Such orders must describe with particularity the communications to be intercepted. 18 U.S.C. § 2518(4)(c).
- To address concerns about particularity, the government must minimize the collection of irrelevant information. 18 U.S.C. § 2518(5).
- There must be clear limits on the time period covered by the surveillance, and the search must end when the government obtains the evidence it seeks. 18 U.S.C. §§ 2518(4)(e), (5).
- The crime being investigated must be an enumerated serious crime. 18

U.S.C. § 2518(3)(a).

- Less intrusive means must be unavailable. 18 U.S.C. § 2518(3)(c).
- The police must return to the court with the fruits of their surveillance, and the required notice to the surveillance target is made by the court rather than left to the police. 18 U.S.C. § 2518(8).

Accordingly, "[The Wiretap Act] does not suffer from the infirmities that the Court found fatal to the statute in *Berger* and to the surveillance in *Katz*." *United States v. Tortorello*, 480 F.2d 764, 775 (2d Cir. 1973), *cert. denied*, 414 U.S. 866 (1973). The SCA, for lack of these safeguards, is just as fatally infirm on its face as the *Berger* statute.

As *Berger* demonstrates, laws can be facially invalidated for lacking essential safeguards that render it invalid in all its applications regardless of the facts. *See Berger*, 388 U.S. at 55, 60; *see also Lanzetta v. New Jersey*, 306 U.S. 451, 453 (1939) (invalidating statute making it a crime to be a gang member) ("If on its face the challenged provision is repugnant to the due process clause, specification of details of the offense intended to be charged would not serve to validate it."). This doctrine is not based on First Amendment overbreadth. In *City of Chicago v. Morales*, 527 U.S. 41 (1999), the Supreme Court, although refusing to apply First Amendment overbreadth doctrine, *id.* at 52-53, found a gang loitering statute facially unconstitutional because it lacked guidelines to prevent arbitrary and discriminatory enforcement and conferred "vast discretion" on the police. *Id.* at 60; *see also Kolender v. Lawson*, 461 U.S. 352, 358 (1983) (invalidating

criminal statute for vagueness because its lack of standards "vest[ed] virtually complete discretion in the hands of the police"). The Supreme Court's facial invalidation of the statute in *Berger* falls squarely within this set of cases.

Berger provides the template for how this Court should address the facial challenge here, not *United States v. Salerno* as the government argues. *See* Gov't Brief at 30-31, *citing United States v. Salerno*, 481 U.S. 739, 745-46 (1987). First, *Salerno*'s "no constitutional application" standard does not accurately reflect the Supreme Court's holdings in this area. *See Janklow v. Planned Parenthood, Sioux Falls Clinic*, 517 U.S. 1174, 1175, n. 1 (1996) (Mem) (citing multiple cases where the Supreme Court has not applied the *Salerno* standard); *see also Women's Medical Professional Corp. v. Voinovich*, 130 F.3d 187, 193 (6th Cir. 1997), *cert. denied*, 523 U.S. 1036 (1998) (refusing to apply *Salerno* in facial challenge to abortion regulations).

More importantly, application of the *Salerno* standard to Fourth Amendment facial challenges leads to absurd and dangerous results. Not only would the *Berger* statute have been found facially constitutional, since in some circumstances individuals may have surrendered an expectation of privacy in their conversations, but even a statute authorizing warrantless searches of *residences* would satisfy the Fourth Amendment, for the same reason. This absurdity becomes clear if one replaces "email accounts" with "homes" or "apartments" when reading the government's brief. To wit:

> Some [homes] are abandoned, as when [a renter] stops paying [rent] and the [lease] is [broken]…. The [hypothetical warrantless search statute] may be applied constitutionally in such cases, and a facial challenge to [that statute] is therefore improper.

Gov't Brief at 33-34. The Fourth Amendment's protections cannot be frustrated by such a strict limitation on facial challenges. This Court should find that the SCA, and in particular the combination of 18 U.S.C. §§ 2703(b)(1)(B)(ii), 2703(d) and 2705, facially violates the Fourth Amendment to the extent it allows the search and seizure of stored email contents without at least prior notice or a probable cause warrant.

CONCLUSION

For the foregoing reasons, the decision of the District Court should be affirmed.

DATED: November 22, 2006

By _____

Kevin S. Bankston
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x 126
Facsimile: (415) 436-9993

Attorneys for Amici Curiae

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,990 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6).

DATED: November 22, 2006

By _____

Kevin S. Bankston
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x 126
Facsimile: (415) 436-9993

Attorneys for Amici Curiae

CERTIFICATE OF SERVICE

I certify that, on this 22nd day of November, 2006, two (2) true and correct copies of Brief of Amici Curiae Electronic Frontier Foundation, ACLU of Ohio Foundation, Inc., American Civil Liberties Union, and Center for Democracy and Technology Supporting the Appellee and Urging Affirmance were served via Federal Express, Overnight Delivery, upon the following:

Gregory G. Lockhart, US Attorney
Donetta D. Wiethe
Benjamin C. Glassman
United States Attorney's Office
221 E. 4th Street, Suite 400
Cincinnati, OH 45202

John H. Zacharia
Nathan P. Judish
U.S. Department of Justice
1301 New York Ave., N.W.
Suite 600
Washington, DC 20005

Martin G. Weinberg, Esq.
20 Park Plaza, Suite 905
Boston, MA 02116

Martin S. Pinales, Esq.
105 W. 4th Street, Suite 920
Cincinnati, OH 45202

And that, pursuant to Fed. R. App. P. 25(a)(2)(B)(ii), said brief was filed by dispatching an original and six paper copies via third-party commercial carrier for delivery to the Clerk of the Court within three calendar days.

_____

Kevin S. Bankston
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333 x 126

Attorney for Amici Curiae

November 22, 2006