

FILED
U.S. DISTRICT COURT
DISTRICT OF COLORADO

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO
2010 APR 13 PM 3:24
GREGORY C. LANGHAM
CLERK

IN RE APPLICATION OF THE
UNITED STATES OF AMERICA
FOR AN ORDER PURSUANT TO
18 U.S.C. § 2703(d)

BY _____ DEP. CLK
Misc. No. 09-Y-080 CBS

**MOTION OF ELECTRONIC FRONTIER FOUNDATION, THE
CENTER FOR DEMOCRACY & TECHNOLOGY, THE CENTER
FOR FINANCIAL PRIVACY AND HUMAN RIGHTS, THE
COMPETITIVE ENTERPRISE INSTITUTE, THE COMPUTER
& COMMUNICATIONS INDUSTRY ASSOCIATION, THE
DISTRIBUTED COMPUTING INDUSTRY ASSOCIATION,
GOOGLE INC., NETCOALITION, THE PROGRESS &
FREEDOM FOUNDATION AND TRUSTE FOR LEAVE TO
FILE BRIEF AS *AMICI CURIAE* OPPOSING THE UNITED
STATES' MOTION TO COMPEL COMPLIANCE WITH THIS
COURT'S 2703(d) ORDER**

Amici Electronic Frontier Foundation ("EFF"), *et. al.* through local counsel, Matthew M. Linton and John R. Mann, submit the following motion for leave to file brief as *amici curiae* opposing the United States' Motion to compel compliance with this Court's 2703(d) order. *Amici* hereby state as follows:

CERTIFICATE OF CONFERRAL

Undersigned counsel Kevin S. Bankston attempted to contact Pegeen D. Rhyne, counsel for the United States on Friday, April 9, 2010, but was

unable reach her and was informed that she would be out of the office through Tuesday, April 12, 2010. Counsel Marc Zwillinger for Yahoo!, Inc., the entity subject to the Motion to Compel, has consented to this filing.

STATEMENT OF INTEREST OF *AMICI CURIAE*

1. 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 14,000 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.

2. The Center for Democracy & 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.

3. The Center for Financial Privacy and Human Rights (“CFPHR”), <http://www.financialprivacy.org>, was founded in 2005 to defend privacy, civil liberties and market economics. The Center is a non-profit human rights and civil liberties organization whose core mission recognizes traditional economic rights as a necessary foundation for a broad understanding of human rights. CFPHR is part of the Liberty and Privacy

Network, a non-governmental advocacy and research 501(c)(3) organization.

4. The Competitive Enterprise Institute is a public interest group dedicated to free enterprise and limited government. We believe that the best solutions come from people making their own choices in a free marketplace, rather than government intervention. Since our founding in 1984, CEI has become a leading national voice on a broad range of regulatory issues, from environmental policy to technology law to risk regulation.

5. The Computer & Communications Industry Association (“CCIA”) is a nonprofit membership organization comprised of a wide range of computer, Internet, information technology, and telecommunications companies. Our members include computer and communications companies, equipment manufacturers, software developers, service providers, re-sellers, integrators, and financial service companies. Together, our members employ almost one million workers and generate nearly \$250 billion in annual revenue. For over thirty years, CCIA has advocated for open markets, open systems, open networks, and full, fair, and open competition. A complete list of CCIA’s current members is available online at www.ccianet.org/members.

6. The Distributed Computing Industry Association (“DCIA”) is a non-profit global trade organization working to commercially advance peer-to-peer (P2P), cloud computing, and related technologies. As part of that mission, it operates voluntary working groups comprised of industry representatives engaging with relevant government agencies to improve the performance of distributed computing software from the perspective of consumer safety and security. With more than 100 Member companies, the DCIA brings together software developers and distributors, content providers, broadband network operators, and service-and-support

companies. In addition to its working groups, the DCIA conducts several industry trade conferences each year, distributes the weekly online newsletter DCINFO, and maintains a database of thousands of articles chronicling industry development at www.dcia.info.

7. Google Inc. (“Google”), is a technology leader focused on improving the ways people connect with information. Google offers a broad range of communication and collaboration tools for its users including Gmail, a web-based email service that permits users to store their email online and to download it to their own computer. As an electronic communications service to the public, Google receives legal process from various state and federal agencies, seeking customer information, including the content of Gmail. As such, Google is directly affected by requests such as the one at issue in this matter.

8. NetCoalition serves as the public policy voice for some of the world’s most innovative Internet companies on the key legislative, administrative, and legal issues affecting the online world. Its members include Amazon.com, Ask, Bloomberg LP, eBay, IAC, Google, Wikipedia, and Yahoo!.

9. The Progress & Freedom Foundation (“PFF”) is a market-oriented think tank that studies the digital revolution and its implications for public policy. Its mission is to educate policymakers, opinion leaders and the public about issues associated with technological change, based on a philosophy of limited government, free markets and individual sovereignty.

10. TRUSTe Privacy Seals help consumers click with confidence by guiding them to trustworthy Web sites. Thousands of Web sites rely on TRUSTe industry best practices to help them make the right decisions about privacy and protecting confidential user information. Forty percent of the

top one hundred Web sites are certified to TRUSTe's leading practices including leading retailers, Apple, eBay, Cabela's, Best Buy, Audible, LeapFrog, Microsoft and Yahoo!. To find out more about TRUSTe, visit <http://www.truste.com>.

DESIRABILITY OF AMICUS BRIEF

11. At issue is whether stored electronic communications are protected by statute or Constitution from warrantless access by law enforcement. Communication in America is in the midst of a technological revolution. Information that individuals formerly conveyed in oral conversations (either face-to-face or over the telephone) or in letters or other physical correspondence is now routinely transmitted using email or other forms of electronic communication. This case is one of the first opportunities for this Court to address the application of the Stored Communications Act and the Fourth Amendment to private information conveyed via these new mediums of communications. Given the extremely significant implications for the privacy of Americans' communications, this Court will benefit from briefing by public interest and industry groups who can inform this Court about the impact on speech and privacy of any decision that it may issue.

12. Additional briefing from EFF and other *amici* may help this Court because we have been instrumental to other courts in cases involving the application of information privacy laws to modern communications technologies. These cases include *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *City of Ontario v. Quon*, 130 S. Ct. 1011 (2009) (cert. granted); *Rehberg v. Paulk*, 2010 WL 816832, at *9 (11th Cir. March 11, 2010) (petition for rehearing or hearing en banc pending) and *In The Matter Of The Application Of The United States Of America For An Order*

Directing A Provider Of Electronic Communication Service To Disclose Records To The Government, affirmed by the district court after briefing by *Amici* EFF and CDT in this case, 2008 WL 4191511 (W.D.Pa. Sep 10, 2008), and currently on appeal to the Third Circuit, Case No. 08-4227.

13. If *Amici* are authorized to file a brief, it will present the following principal arguments:


- Yahoo! is correct that 18 U.S.C. § 2703 of the Stored Communications Act requires the government to get a search warrant to obtain access to a Yahoo! user's emails that are no more than 180 days old, even if the user may have opened those messages.
- Moreover, the Fourth Amendment protects stored emails just as it does conversational privacy and private papers.
- This Court must protect the user's privacy in these emails by requiring the government to seek and obtain a search warrant based on probable cause, either by interpreting the SCA correctly and finding that opened messages are "in electronic storage" or by finding that users have a constitutionally protected reasonable expectation of privacy in their stored communications.

14. Because of the importance of the issues raised herein, and the far reaching effects upon litigants and national email providers, *Amici* respectfully request that they be permitted to appear herein as *Amici Curiae*, and to file their Brief opposing the United States' Motion to compel compliance with this Court's 2703(d) order.

15. *Amici* hereby conditionally file the accompanying Brief of *Amici Curiae* simultaneously with this Motion for Leave.

WHEREFORE, *Amici* EFF, *et. al.* respectfully requests that the Court grant them leave to file their brief as *Amici Curiae* opposing the United States' motion to compel, and that the Court accept the brief of *Amici Curiae* which is conditionally filed with this Motion for Leave.

DATED: April 13, 2010

By 

Matthew M. Linton
mlinton@kcfpc.com
John R. Mann
jmann@kcfpc.com
KENNEDY CHILDS & FOGG, P.C.
633 17th Street, Suite 2200
Denver, Colorado 80265
PHONE: (303) 825-2700
FAX: (303) 825-0434

LOCAL COUNSEL FOR *AMICI CURIAE*

Kevin S. Bankston (*application for admission forthcoming*)
bankston@eff.org
Jennifer Granick (*application for admission forthcoming*)
jennifer@eff.org
ELECTRONIC FRONTIER
FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
PHONE: (415) 436-9333
FAX: (415) 436-9993

ATTORNEYS FOR *AMICI CURIAE*

Paul Ohm (*application for admission forthcoming*)
paul.ohm@colorado.edu

SAMUELSON-GLUSHKO
TECHNOLOGY LAW & POLICY
CLINIC
University of Colorado Law School
401 UCB
Boulder, CO 80309
PHONE: (303) 492-0384
FAX: (303) 492-1200

ATTORNEY FOR *AMICI CURIAE*

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

IN RE APPLICATION OF THE
UNITED STATES OF AMERICA
FOR AN ORDER PURSUANT TO
18 U.S.C. § 2703(d)

Misc. No. 09-Y-080 CBS

**BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER
FOUNDATION, THE CENTER FOR DEMOCRACY &
TECHNOLOGY, THE CENTER FOR FINANCIAL PRIVACY
AND HUMAN RIGHTS, THE COMPETITIVE ENTERPRISE
INSTITUTE, THE COMPUTER & COMMUNICATIONS
INDUSTRY ASSOCIATION, THE DISTRIBUTED COMPUTING
INDUSTRY ASSOCIATION, GOOGLE INC., NETCOALITION,
THE PROGRESS & FREEDOM FOUNDATION AND TRUSTE
OPPOSING THE UNITED STATES' MOTION TO COMPEL
COMPLIANCE WITH THIS COURT'S 2703(d) ORDER**

STATEMENT OF *AMICI CURIAE*

Amici are a collection of non-profit public interest and advocacy organizations, Internet companies and industry associations seeking to ensure the preservation of Fourth Amendment and statutory privacy protections for advancing communications 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 14,000 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, <http://www.eff.org>.

The Center for Democracy & 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.

The Center for Financial Privacy and Human Rights (“CFPHR”), http://www.financial_privacy.org, was founded in 2005 to defend privacy, civil liberties and market economics. The Center is a non-profit human rights and civil liberties organization whose core mission recognizes traditional economic rights as a necessary foundation for a broad understanding of human rights. CFPHR is part of the Liberty and Privacy Network, a non-governmental advocacy and research 501(c)(3) organization.

The Competitive Enterprise Institute is a public interest group dedicated to free enterprise and limited government. We believe that the best solutions come from people making their own choices in a free marketplace, rather than government intervention. Since our founding in 1984, CEI has become a leading national voice on a broad range of regulatory issues, from

environmental policy to technology law to risk regulation.

The Computer & Communications Industry Association (“CCIA”) is a nonprofit membership organization comprised of a wide range of computer, Internet, information technology, and telecommunications companies. Our members include computer and communications companies, equipment manufacturers, software developers, service providers, re-sellers, integrators, and financial service companies. Together, our members employ almost one million workers and generate nearly \$250 billion in annual revenue. For over thirty years, CCIA has advocated for open markets, open systems, open networks, and full, fair, and open competition. A complete list of CCIA’s current members is available online at <http://www.ccianet.org/members>.

The Distributed Computing Industry Association (“DCIA”) is a non-profit global trade organization working to commercially advance peer-to-peer (P2P), cloud computing, and related technologies. As part of that mission, it operates voluntary working groups comprised of industry representatives engaging with relevant government agencies to improve the performance of distributed computing software from the perspective of consumer safety and security. With more than 100 Member companies, the DCIA brings together software developers and distributors, content providers, broadband network operators, and service-and-support companies. In addition to its working groups, the DCIA conducts several industry trade conferences each year, distributes the weekly online newsletter DCINFO, and maintains a database of thousands of articles

chronicling industry development at <http://www.dcia.info>.

Google Inc. (“Google”), is a technology leader focused on improving the ways people connect with information. Google offers a broad range of communication and collaboration tools for its users including Gmail, a web-based email service that permits users to store their email online and to download it to their own computer. As an electronic communications service to the public, Google receives legal process from various state and federal agencies, seeking customer information, including the content of Gmail. As such, Google is directly affected by requests such as the one at issue in this matter.

NetCoalition serves as the public policy voice for some of the world’s most innovative Internet companies on the key legislative, administrative, and legal issues affecting the online world. Its members include Amazon.com, Ask, Bloomberg LP, eBay, IAC, Google, Wikipedia, and Yahoo!.

The Progress & Freedom Foundation (“PFF”) is a market-oriented think tank that studies the digital revolution and its implications for public policy. Its mission is to educate policymakers, opinion leaders and the public about issues associated with technological change, based on a philosophy of limited government, free markets and individual sovereignty.

TRUSTe Privacy Seals help consumers click with confidence by guiding them to trustworthy Web sites. Thousands of Web sites rely on TRUSTe industry best practices to help them make the right decisions about

privacy and protecting confidential user information. Forty percent of the top one hundred Web sites are certified to TRUSTe's leading practices including leading retailers, Apple, eBay, Cabela's, Best Buy, Audible, LeapFrog, Microsoft and Yahoo!. To find out more about TRUSTe, visit <http://www.truste.com>.

INTRODUCTION AND SUMMARY OF ARGUMENT

The government seeks to compel Yahoo! to turn over the contents of one of its user's email accounts without a search warrant and based on a showing only that the information is relevant and material to the government's investigation. Because the emails have been opened, the government asserts they are no longer electronic communications in "electronic storage" and receive less privacy protection than do unread emails. The user apparently has not been notified of this request, but Yahoo! has opposed it because the disclosure would be contrary to the weight of precedent and would improperly violate its customer's constitutional rights.

Yahoo! is correct that 18 U.S.C. § 2703 of the Stored Communications Act ("SCA") requires the government to get a search warrant to obtain access to a Yahoo! user's emails that are no more than 180 days old, even if the user may have opened those messages. This is the only conclusion consistent with the plain language of the statute, relevant case law, and the legislative history. Moreover, the Fourth Amendment protects stored emails just as it does conversational privacy and private papers. The mere fact that a service provider has the ability to access email messages

does not defeat the user's expectation of privacy in their contents, just as the fact that telephone wires lead outside the home does not extinguish the Fourth Amendment rights of those talking over the telephone lines, and just as the fact that one has a roommate or is renting a room does not defeat Fourth Amendment protection in one's home or hotel room.

This Court must protect the user's privacy in these emails by requiring the government to seek and obtain a search warrant based on probable cause, either by interpreting the SCA correctly and finding that opened messages are "in electronic storage" or by finding that users have a constitutionally protected reasonable expectation of privacy in their stored communications.

ARGUMENT

I. THE STORED COMMUNICATIONS ACT REQUIRES THE GOVERNMENT TO OBTAIN A SEARCH WARRANT FOR THE EMAILS IT SEEKS.

Section 2703 of the Stored Communications Act ("SCA") plainly requires the government to obtain a search warrant in order to compel Yahoo!'s disclosure of emails no more than 180 days old, which are in "electronic storage" and therefore strongly protected by the statute regardless of whether they are opened or unopened. *See* 18 U.S.C. § 2703(a) (requiring a warrant before the government may obtain communications contents in "electronic storage" with an electronic communication service provider for 180 days or less); *Theofel v. Farey-Jones*, 341 F.3d 978, 985 (9th Cir. 2003) (finding that opened emails stored by a provider for backup purposes of the provider or the user are in "electronic storage"). The

government's strained reading of the SCA to allow access to these messages without a warrant contradicts the statute's plain language, the existing case law, and the SCA's privacy-protective purpose, and should be rejected by this Court. *See* Yahoo! Br. at Section I.¹

II. THE FOURTH AMENDMENT REQUIRES THE GOVERNMENT TO OBTAIN A SEARCH WARRANT TO COMPEL PRODUCTION OF THE EMAILS IT SEEKS.

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

1. Under Supreme Court Precedent Applying the Fourth Amendment to Telephone Conversations, Email Users Possess a Reasonable Expectation of Privacy in the Contents of Emails Stored with an Email Service Provider.

Under the reasoning of *Katz v. United States*, 389 U.S. 347 (1967), which is the touchstone of modern Fourth Amendment doctrine, email users have a constitutionally protected “reasonable expectation of privacy” in their stored email messages. *See id.* at 360-61 (Harlan, J., concurring). Fourth

¹ In addition, the doctrine of constitutional avoidance leads to this construction, as it is the only reading of the statute that would allow the Court to avoid the serious constitutional question surrounding the Fourth Amendment's application to email. That doctrine “rest[s] on the reasonable presumption that Congress did not intend” any meaning of a statute “which raises serious constitutional doubts,” *Clark v. Martinez*, 543 U.S. 371, 381 (2005), and “[i]t is therefore incumbent upon [the Court] to read the statute to eliminate those doubts so long as such a reading is not plainly contrary to the intent of Congress.” *United States v. X-Citement Videos, Inc.*, 513 U.S. 64, 78 (1994); *see also United States ex rel. Attorney General v. Delaware & Hudson Co.*, 213 U.S. 366, 407-08 (1909).

Amendment protections apply where “a person [has] exhibited an actual (subjective) expectation of privacy . . . that society is prepared to recognize as [objectively] ‘reasonable.’” *Id.* The reasonableness of an expectation of privacy in the contents of stored emails is directly analogous to society’s constitutionally-protected expectations of privacy in the contents of phone calls.

The Supreme Court in *Katz* held that “the Fourth Amendment protects people, not places.” *Id.* at 351 (majority opinion). 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 protected by the Fourth Amendment against search or seizure by the government. *Compare id. with 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). In *Katz*, the Supreme Court 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 is to ignore the vital role that the public telephone has come to play in private communication.”). In 1967, society’s reliance on public telephones for private communication established both the subjective expectation that phone calls were private as well as the objective reasonableness of that

expectation, giving rise to Fourth Amendment protection. *See id.*

Since *Katz*, the Supreme Court has looked regularly to societal expectations when applying the Fourth Amendment, particularly when scrutinizing new technologies. *See Georgia v. Randolph*, 547 U.S. 103, 111 (2006) (finding 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) (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").

Based on society's extensive use of email for private, sensitive communications, it is plain that email plays at least as vital a role in private communication today that the public telephone played in 1967, and that society expects and relies on the privacy of email messages just as it relies on the privacy of the telephone system.² It is equally plain that society expects privacy in its *stored* email messages: email users often store many if not all of their personal messages with the provider after they have been sent

² As of 2003, more than 100 million Americans used email, and "more than nine in ten online Americans have sent or read email." Pew Research Center, *America's Online Pursuits*, available at <http://www.pewinternet.org/Reports/2003/Americas-Online-Pursuits.aspx> (last visited Apr. 11, 2010). By 2008, the majority of Internet users (56%) were using webmail, where the messages are stored with the service provider. Pew Research Center, *Use of Cloud Computing Applications and Services*, <http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx> (last visited Apr. 11, 2010).

or received, rather than downloading them onto their own computers. See *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1005 (9th Cir. 2009) (en banc) (Noting that “many people no longer keep their email primarily on their personal computer, and instead use a web-based email provider, which stores their messages along with billions of messages from and to millions of other people.”). Indeed, the largest email services are popular precisely because they offer users huge amounts of computer disk space in the Internet “cloud” within which users can warehouse their emails for perpetual storage.³ In light of these societal patterns, to hold that the hundreds of millions of people who store their email messages with providers such as Yahoo! or Microsoft or Google lack either a subjective or objective expectation of privacy makes no sense, and would plainly violate *Katz* by failing to protect society’s expectations of privacy.

The Supreme Court’s decision in *Smith v. Maryland*, 442 U.S. 735 (1979), reaffirmed and clarified *Katz*’s holding that the Fourth Amendment protects the contents of private communications such as email. The *Smith* court distinguished the contents of phone calls, which it reaffirmed are

³ For example, Google’s “Gmail” service currently offers over 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> (last visited Apr. 11, 2010); see also Google, *Getting Started with Gmail*, available at <http://mail.google.com/mail/help/intl/en/start.html> (last visited Apr. 11, 2010) (“**Don’t waste time deleting messages** [T]he typical user can go for years without deleting a single message.”) (emphasis in original).

protected by the Fourth Amendment under *Katz*, from the dialed phone numbers acquired by “pen register” surveillance, which it held are not protected. *Id.* at 741-42.⁴ *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). Despite the fact that the electrical impulses constituting the contents of a telephone conversation are just 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). 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)). In other words, *Smith* held that *Miller*’s “assumption-of-risk” analysis does not extend to communications content protected under *Katz*, and confirmed that spying on what callers are saying is

⁴ *Amici* do not necessarily agree 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.

more invasive than knowing what phone numbers they are dialing. *See Smith*, 442 U.S. at 741 (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))).

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 rather constitutes one’s private papers and effects. As the *Miller* court explained in distinguishing *Katz*, “the documents subpoenaed [were] not respondent’s ‘private papers’” nor his “confidential communications,” and the “respondent [could] assert neither ownership nor possession [of the documents]. Instead, these [were] *the business records of the banks*,” which “pertain[ed] to transactions to which the bank was itself a party” and “contain[ed] only information . . . exposed to [the bank’s] employees in the ordinary course of business.” *Miller*, 425 U.S. at 440-42 (emphasis added).

In contrast, the eavesdropping in *Katz* constituted a search and seizure of Katz’s intangible conversations, which were constitutionally akin to his tangible papers and effects. *See Katz*, 389 U.S. at 353 (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 reaffirmed many times that under the Constitution, conversations are like papers and effects, not mere

business records. See *Berger v. New York*, 388 U.S. 41, 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)); *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.”). These cases confirm that the Fourth Amendment protects *the content of private conversations*, whether tangible or intangible and regardless of whether transmitted over the telephone system or the Internet.

Finally, the conclusion that the Fourth Amendment protects stored email is also supported by analogy to the expectation of privacy in the contents of sealed postal mail and in the contents of hotel rooms and other rented properties. The Supreme Court has recognized an expectation of privacy in the contents of sealed packages and letters even though carried by a third party. See *Ex Parte Jackson*, 96 U.S. 727, 733 (1878). Bank customers expect privacy in the contents of their safe deposit boxes, even though stored by a third party. See *United States v. Thomas*, No. 88-6341, 1989 WL 72926, at *2 (6th Cir. July 5, 1989). Finally, tenants in rented residences and hotel rooms maintain Fourth Amendment privacy in their

units while they occupy them. *See Stoner v. California*, 376 U.S. 483, 489 (1964). The fact that the property owners and their employees may be entitled to enter the premises to repair damage or provide agreed-upon services, analogous to the “spam” and computer virus filtering often provided by email services such as Yahoo!, does nothing to diminish the tenant’s expectations against the government. *Id.*

2. Following Supreme Court Precedent, Judges and Scholars Have Regularly Concluded That Email Users Possess A Reasonable Expectation of Privacy in the Contents of Emails Stored With An Email Provider.

Looking to the clear lesson of *Katz* and *Smith*, a long line of judges and legal scholars have concluded that the Fourth Amendment protects stored email messages. Two federal, military appellate courts have come to this conclusion, affording Fourth Amendment protection to email messages, despite the role of third-party email providers in storing these messages. *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 agreed. A judge in the District of Rhode Island has held that users possess Fourth Amendment rights in email accounts operated by private providers. *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”). Another judge in the Eastern District of New York has ruled that the numbers dialed on a telephone *after* a call has been initiated—numbers like account numbers sent to a bank or the password and

commands sent to a voice mail system—are protected contents under *Katz*, and distinguishable from unprotected numbers dialed to initiate a call under *Smith*. *In re Applications of U.S. for Orders Authorizing the Use of Pen Registers and Trap and Trace Devices*, 515 F. Supp. 2d 325, 336 (E.D.N.Y. 2007). Similarly, a judge the District of Massachusetts found Fourth Amendment protection in the contents of a password-protected website. *United States v. D’Andrea*, 497 F. Supp. 2d 117 (D. Mass. 2007).

Importantly, none of these judges applied the assumption of risk rationale of *Miller* to email. 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.

In re Applications of U.S., 515 F. Supp. 2d at 338 (citations removed).

Courts of Appeal have concurred. Both the Sixth and Ninth Circuits have directly extended Fourth Amendment protection to the contents of electronic communications, albeit in one opinion that was vacated on other grounds and another that is currently being reviewed by the Supreme Court. First, in *Warshak v. United States (Warshak I)*, 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 email, 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 societal expectation that the ISP or the phone company will not do so as a matter of course.” *Id.* at 471 (emphasis in original). 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, 905 (9th Cir. 2008).

Although both of these opinions have now been vacated—*Warshak* as not ripe, *Warshak v. United States*, 532 F.3d 521, 523 (6th Cir. 2008), *Quon* by the Supreme Court upon its grant of certiorari, *City of Ontario v. Quon*, 130 S. Ct. 1011 (2009)—both cases are nevertheless persuasive precedents. *Warshak* provides a detailed and careful explanation why email contents are constitutionally protected. *Quon* directly applies the Ninth Circuit’s earlier reasoning in *United States v. Forrester*, 495 F.3d 1041 (9th Cir. 2007), which is still good law. In *Forrester*, the Ninth Circuit expressly analogized electronic mail—with its non-private addressing information and its private contents—to physical mail. *Id.* at 1049 (“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.”).

Even more recently, the Eleventh Circuit recognized the Fourth Amendment distinction between the contents of communications that are expected to remain private and non-content information that is voluntarily exposed to a communications provider. *See 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) (emphasis added).⁵

Finally, courts have found important expectations of privacy in email

⁵ In another opinion published just two days after *Beckett*, a different panel of the Eleventh Circuit threatened to upset the consensus that the content of electronic communications are protected by the Fourth Amendment, by conflating email *content* with email *records* when holding that, “[l]acking a valid expectation of privacy in that *email information*, Rehberg fails to state a Fourth Amendment violation for the subpoenas for his *Internet records*.” *Rehberg v. Paulk*, No. 09-11897, 2010 WL 816832, at *9 (11th Cir. Mar. 11, 2010) (emphasis added). *Amicus* Electronic Frontier Foundation, representing the plaintiff, petitioned last month for a rehearing in that case (petition available at http://www.eff.org/files/filenode/rehberg_v_hodges/rehbergmotion.pdf, last accessed Apr. 11, 2010).

outside of the Fourth Amendment context. For example, several courts have extended the attorney-client privilege to email messages, finding both subjective and objective expectations of privacy and explaining why the provider's ability to access the messages did not produce a different result. *See, e.g., Stentgart v. Loving Care Agency, Inc.*, A-16-09, 2010 N.J. LEXIS 241, *38-39 (N.J. Mar. 30, 2010) ("Under all of the circumstances, we find that Stentgart 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) (finding, in the attorney-client privilege context, that a user "had a reasonable subjective and objective belief that his [Hotmail] communications would be kept confidential").

In addition to the growing consensus in the courts, a growing number of legal scholars have concluded that users have a reasonable expectation of privacy in the contents of electronic mail messages. *See, e.g.,* Patricia L. Bellia & Susan Freiwald, *Law in a Networked World: Fourth Amendment Protection for Stored Email*, 2008 U. Chi. Legal F. 121, 135-140; Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, Stan. L. Rev. (forthcoming 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) (“Therefore, as with postal mail and telephone conversations, the sender of e-mail retains no REP [reasonable expectation of privacy] in the addressing components, but should retain a REP in the contents.”). *Amici* know of no legal scholars who have concluded otherwise.

In sum, many of our most important private conversations have migrated from the telephone network and the sealed envelope to the email server, and the Supreme Court’s repeated holdings about conversational privacy should apply directly to this new medium. *Katz* and *Smith* require that this Court afford stored email the same protection as private conversations, papers and effects.

3. Yahoo!’s Privacy Policy and Terms of Service Support Rather than Undermine Users’ Reasonable Expectation of Privacy in Their Emails.

To the extent the government contends that Yahoo!’s privacy policy and terms of service eliminate users’ expectation of privacy in their emails, the Court should decline that invitation “to make a crazy quilt of the Fourth Amendment” by allowing its protections to be dictated by the “practices of a private corporation.” *See Smith*, 442 U.S. at 745. Basic constitutional rights should not turn on the wording of a particular email provider’s agreements with its users. However, to the extent the Court does consider those notices, they clearly support rather than undermine Yahoo! email users’ privacy expectations.

Email providers like Yahoo! routinely supplement their users’ expectation of privacy via official “privacy policies” that delineate the

providers' limited authority to access stored email. For example, Yahoo!'s Privacy Policy reassures users that:

Yahoo! takes your privacy seriously.... We limit 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. We have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you.

Yahoo!, *Yahoo! Privacy Policy*, available at <http://privacy.yahoo.com/> (last visited Apr. 11, 2010) (emphasis in original); *see also*, e.g., Google, *Google Privacy Policy*, available at <http://www.google.com/privacypolicy.html> (last visited Apr. 11, 2010) (“At Google we recognize that privacy is important Google only processes personal information for the purposes described in this Privacy Policy”). These representations belie any claim by the government that providers have “unlimited access” to stored email that eliminates constitutional protections, and instead only add to the reasonableness of email users’ expectation of privacy.

Yahoo!'s Terms of Service further bolster an expectation of privacy by disclaiming any ownership interest in its users’ emails. *See* Yahoo!, *Yahoo! Terms of Service*, available at <http://docs.yahoo.com/info/terms/> (last visited Apr. 11, 2010) (“Yahoo! does not claim ownership of Content you submit or make available for inclusion on the Yahoo! services.”). Thus, the emails in this case are entirely unlike the records in *Miller*, which were “not respondent’s ‘private papers’” nor his “confidential communications” but instead were “*the business records of the banks*,” and the “respondent

[could] assert neither ownership nor possession [of the documents].” *Miller*, 425 U.S. at 442 (emphasis added).

The mere fact that a privacy policy or term of service may allow for some level of access to a user’s emails is not enough to undermine the constitutionally protected expectation of privacy. The fact that others may have occasional access to a computer does not automatically eliminate Fourth Amendment protection for others that use that computer. *Leventhal v. Knapek*, 266 F.3d 64, 73-74 (2d Cir. 2001) (holding that public employee had a reasonable expectation of privacy in the contents of his office computer). Nor do policies that allow limited access to private content in order to maintain the security and integrity of the provider’s systems. *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007) (University policy reserving right to access student computers to protect rights and property did not undermine reasonable expectation of privacy or Fourth Amendment protection).

Rather, as *Katz*, *Smith*, and *New York Tel. Co.* make clear, neither a provider’s limited ability to access communications nor its occasional use of that ability is relevant to the customer’s expectation of privacy in the *contents* of those 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, at common law, they have impliedly consented to eavesdropping by the phone company that is reasonably necessary to effectively maintain the phone 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). 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, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that 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 this limited access and disclosure—or a subscriber’s implied consent to it—negates the subscriber’s expectation of privacy in the contents of her communications.

Yahoo!’s terms of service describing when it may voluntarily access

or disclose Yahoo! customers' email track the existing provider exception, and like that exception focus on Yahoo!'s ability to render service and protect its rights and property:

You acknowledge, consent and agree that Yahoo! may access, preserve and disclose your account information and Content if required to do so by law or in a good faith belief that such access preservation or disclosure is reasonably necessary to: (i) comply with legal process; (ii) enforce the TOS; (iii) respond to claims that any Content violates the rights of third parties; (iv) respond to your requests for customer service; or (v) 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 Apr. 11, 2010). This is exactly the type of limited access by the provider that was and is irrelevant under *Katz's* and *Heckenkamp's* reasoning.

Consequently, neither the potential exposure of stored email to Yahoo!'s system administrators in the course of their regular duties, nor Yahoo!'s use of software filters to screen out junk email and emails containing viruses, eliminates an email user's expectation of privacy. To hold otherwise would pose a constitutional Catch-22 that ignores the vital role that email and the Internet as a whole play 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

unsolicited “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.

B. **THE FOURTH AMENDMENT REQUIRES THE GOVERNMENT TO OBTAIN A SEARCH WARRANT BEFORE INVADING AN EMAIL USER’S REASONABLE EXPECTATION OF PRIVACY.**

The government may not circumvent the warrant requirement and avoid a probable cause showing by using a § 2703(d) order to compel the disclosure of email communications that are reasonably expected to be private. No case law supports the dangerous proposition that a mere showing of relevance to compel disclosure of stored private emails from an email provider satisfies the Fourth Amendment. Cases such as *United States v. Miller* that allowed subpoenas to compel the production of business records that were not reasonably expected to be private are inapposite because Yahoo!’s email users do possess a reasonable expectation of privacy in their emails, which are their private documents and not the business records of Yahoo!. *See supra* at Section II.A. The usual Fourth Amendment rule requiring a search warrant based on probable cause for unnoticed searches and seizures of private materials applies.

The government argued in *Warshak* for a *per se* rule where compelled

disclosures only ever require reasonableness, as opposed to the probable cause required for a warrant. Yet, as the law professor *amici* demonstrated in their brief in *Warshak* and in later legal scholarship, courts have upheld the use of subpoenas to obtain records only after first finding no reasonable expectation of privacy in the materials sought. See Patricia L. Bellia & Susan Freiwald, *The Fourth Amendment Status of Stored E-Mail: The Law Professors' Brief in Warshak v. United States*, 41 U.S.F. L. Rev. 559, 579-85 (2007); Bellia & Freiwald, *Law in a Networked World*, *supra*, at 141-47. For example, the Supreme Court in *Miller* needed to address whether there was an expectation of privacy in bank records before holding that the subpoenas in that case satisfied the Fourth Amendment. See *Miller*, 425 U.S. at 440-43; see also *Warshak I*, 490 F.3d at 474 (discussing *Miller* and similar cases where courts have upheld the constitutionality of subpoenas only after finding no reasonable expectation of privacy in the subpoenaed materials); Bellia & Freiwald, *Law in a Networked World*, *supra*, 143-46 (same). Thus, the government's assertion that it may compel disclosure of stored emails from an email provider upon a showing that the information is relevant and material to the investigation, regardless of an email user's reasonable expectation of privacy, is mistaken.

Courts' careful consideration of the reasonable expectation of privacy question before allowing compelled disclosure via subpoena demonstrates that a subpoena compelling the disclosure of, *e.g.*, "a personal diary" would raise "[s]pecial problems of privacy" not raised by a subpoena for a third

party's financial records. *See Fisher v. United States*, 425 U.S. 391, 401 n.7 (1976). Those special problems of privacy are squarely presented here, and may only be overcome by the same showing of probable cause that is ordinarily required when the government wants to search and seize personal documents or communications. As the court in *Warshak I* held in analogous circumstances,

The government's compelled disclosure argument . . . begs the critical question of whether an e-mail user maintains a reasonable expectation of privacy in his e-mails If he does not . . . then the government must meet only the reasonableness standard applicable to compelled disclosures to obtain the material. If, on the other hand, the e-mail user *does* maintain a reasonable expectation of privacy in the content of the e-mails . . . then the Fourth Amendment's probable cause standard controls the e-mail seizure.

Warshak I, 490 F.3d at 469 (emphasis added). In other words, where there is an expectation of privacy in the subpoenaed email, "subpoenaing the entity with mere custody over the documents is insufficient to trump the Fourth Amendment warrant requirement." *Id.* at 475.

This conclusion is bolstered by the fact that the email user in this case apparently has not been notified of the Court's § 2703(d) order and thus has not had any opportunity to respond to it. From the perspective of the email service user, which the Court must bear in mind is the relevant perspective here, *see Stoner*, 376 U.S. at 489 (propriety of search depends on rights of hotel guest, not proprietor), the government's acquisition of stored email without notice or an opportunity to be heard is indistinguishable from a search or seizure under the Fourth Amendment. Absent notice and

opportunity to be heard, however, the compelled disclosure of materials in which the target has a reasonable expectation of privacy are simply searches and seizures by another name. *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.”); *see also King v. State*, 535 S.E.2d 492, 497 (Ga. 2000) (holding that subpoena violated state constitution “because Ms. King did not have notice and an opportunity to object to the State’s subpoena of her medical records in which she had not waived her right of privacy.”). *See also In re Nwamu*, 421 F. Supp. 1361 (S.D.N.Y. 1976), where FBI agents armed with a grand jury subpoena seized items immediately as if the subpoena 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.

Hence, on facts essentially identical to this case, the *Warshak I* court found that lack of prior notice to the email user was fatal to the constitutionality of the § 2703(d) order at issue there. *See Warshak I*, 490

F.3d at 475, citing *United States v. Phibbs*, 999 F.2d 1053, 1077 (6th Cir. 1993). So too should this Court reject the government's attempted end-run around the Fourth Amendment and instead require it to obtain a search warrant based on probable cause before searching and seizing emails without prior notice to the account holder.⁶

C. **THIS COURT HAS THE AUTHORITY AND THE OBLIGATION TO ENSURE THAT ITS ORDERS COMPLY WITH THE FOURTH AMENDMENT.**

Amici agree that Yahoo! has standing to assert the Fourth Amendment rights of its email users. *See* Yahoo! Br. at Section II. Such standing is necessary to protect the user's Fourth Amendment rights even when the targeted email account-holder is ignorant of the current controversy and unable to press his or her own rights. Courts in analogous situations have found that Internet service providers and other third parties have standing to raise the constitutional rights of their customers. *See, e.g., In re Verizon*

⁶ Importantly, any order this Court issues compelling the disclosure of the Yahoo! emails should not reach every email in the targeted account, but must instead satisfy the Fourth Amendment's particularity requirement and reasonably narrow the scope of the demand to only those emails that are relevant to the government's investigation. *See Warshak I*, 490 F.3d at 476 n.8; *see also United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d at 998 (discussing special warrant procedures that are necessary "to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases"), at 1005 (specifically discussing email) and at 1006 (outlining special procedures that magistrates must follow when issuing warrants or subpoenas in order to satisfy the Fourth Amendment in "digital evidence cases").

Internet Services, Inc., 257 F. Supp. 2d 244 (D.D.C. 2003), *rev'd on other grounds, Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir. 2003) (Internet service provider had standing to challenge subpoena based on First Amendment rights of its customers); *Mia Luna, Inc. v. Hill*, No. 1:08-CV-585, 2008 WL 4002964 at *6-8 (N.D. Ga. Aug. 22, 2008) (adult entertainment venue had standing to raise Fourth Amendment rights of customers when challenging police roadblocks alleged to have been set up for the express purpose of hindering the venue's patrons); *see also McVicker v. King*, 02: 09-cv-00436, 2010 WL 786275 at *4 (W.D. Pa. Mar. 3, 2010) (noting that "[t]he trend among courts which have been presented with this question is to hold that entities such as newspapers, Internet service providers, and website hosts may, under the principle of *jus tertii* standing, assert the rights of their readers and subscribers").

Regardless of Yahoo!'s standing, however, this Court also has the inherent authority and the obligation under Article III to ensure that the orders it issues are in accordance with the law, including the Constitution. *See Young v. United States ex rel. Vuitton et Fils S.A.*, 481 U.S. 787, 816 (1987) (Scalia, J., concurring) ("The judicial power is the power to decide, *in accordance with law*, who should prevail in a case or controversy") (emphasis added); *see also The Federalist No. 39*, at 233 (James Madison) (Garry Wills ed., 2003) (explaining that decisions of federal courts are "to be impartially made, *according to the rules of the Constitution*; and all the usual

and most effectual precautions are taken to secure this impartiality”) (emphasis added); James S. Liebman & William F. Ryan, “*Some Effectual Power*”: *The Quantity and Quality of Decisionmaking Required of Article III Courts*, 98 Colum. L. Rev. 696, 771 (1998) (concluding, after exhaustively combing the records of the Constitutional Convention and analyzing two centuries of federal court decisions, that “[T]he judicial Power’ means the Article III judge’s authority *and obligation*, in all matters over which jurisdiction is conferred, independently, finally, and effectually to decide the whole case and nothing but the case on the basis, and so as to maintain the supremacy, of the whole federal law.” (emphasis added)).

The Article III judicial power delegated to Court does not authorize anything beyond what the Constitution allows, and requires the Court to consider the limits of the Fourth Amendment when judging an *ex parte* application by the government to intrude on an individual’s privacy. Failure to consider the Fourth Amendment in this case would undermine the Judiciary’s role in protecting individuals against unconstitutional searches and seizures. *See United States v. Jeffers*, 342 U.S. 48, 51 (1951) (“Over and again this Court has emphasized that the mandate of the Amendment requires adherence to judicial processes.”); *United States v. United States District Court (Keith)*, 407 U.S. 297, 317 (1972) (“This judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government.”).

It is of no import that the email user whose Fourth Amendment rights are at issue is not currently before the Court. Indeed, courts routinely consider the Fourth Amendment rights of parties not before the court in the context of *ex parte* law enforcement requests, not only and most obviously when the government seeks a search warrant but also in the context of § 2703(d) requests. Recently, for example, a federal magistrate judge in Pittsburgh relied in part on the Fourth Amendment when denying an application for a § 2703(d) order compelling a cell phone company's disclosure of a subscriber's cell phone location information. *See In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 534 F. Supp. 2d 585 (W.D. Pa. 2008). That decision was affirmed by the district court after briefing by several of the *Amici* in this case, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), and is currently on appeal to the Third Circuit.⁷

Like the Third Circuit Court of Appeals, other magistrates and district court judges have recently considered the Fourth Amendment issues raised by similar *ex parte* applications by the government, even though the targets were not before the court. *See, e.g., In re Applications of U.S. for Orders*

⁷ A recording of the Third Circuit's Feb. 12, 2010 oral argument in that case (No. 08-4227), where a substantial portion of the questions to government and *amici* concerned the Fourth Amendment, is available on the Circuit Court's web site at <http://www.ca3.uscourts.gov/oralargument/audio/08-4227-ApplicationofUSA.wma> (last visited Apr. 11, 2010).

Authorizing the Use of Pen Registers, 515 F. Supp. 2d at 339 (rejecting on Fourth Amendment grounds a government application for an order authorizing pen register surveillance); *In re Application of U.S. for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device or Process*, 441 F. Supp. 2d 816, 836-87 (S.D. Tex. 2006) (applying constitutional avoidance and construing statute to deny government requests to conduct pen register surveillance and track the location of a cell phone, noting that “[t]he Government’s requests raise Fourth Amendment warning flags, which threaten heavy weather if either were to be allowed”); and *In re Applications of U.S. for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices*, 632 F. Supp. 2d 202, 208-10 (E.D.N.Y. 2008) (granting order authorizing location tracking of a cell phone but only after considering Fourth Amendment arguments raised by *Amici*, and noting that “applications under the Pen Register Statute and the SCA . . . directly implicate Fourth Amendment concerns”).

Whether raised by Yahoo!, by *Amici*, or *sua sponte* by the Court, the question of whether the requested order complies with the Fourth Amendment should be addressed by the Court. The SCA itself was in part an attempt by Congress to protect Fourth Amendment rights where those rights may be unclear due to changing technologies.⁸ In passing the SCA

⁸ As the Senate Judiciary Committee’s report explained,

With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of

and allowing for email providers like Yahoo! to move to quash or modify § 2703(d) orders, Congress revealed its intention that judges would continue to play their familiar role as guardians of the Constitution, and the Fourth Amendment in particular, in this context.

There may have been a lack of clarity in 1986 about the Fourth Amendment status of stored email, but there is none today, *see supra* at Section II. This Court should consider the Fourth Amendment's requirements in spite of the absence of the user in this proceeding. Indeed, the importance is heightened here where the user is unable to raise such arguments in this *ex parte* proceeding.

CONCLUSION

For the foregoing reasons, the government's motion to compel Yahoo!'s compliance with the § 2703(d) order should be denied.

personal and business information For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection.

S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557; *see also, e.g., Oversight on Communications Privacy: Hearing on Privacy in Electronic Communications Before the Subcomm. on Patents, Copyrights, and Trademarks of the S. Comm. on the Judiciary, 98th Cong. 17 (1984)* ("In this rapidly developing area of communications which range from cellular non-wire telephone communications to microwave-fed computer terminals, distinctions such as [whether a participant to an electronic communication can claim a reasonable expectation of privacy] are not always clear or obvious.").

DATED: April 13, 2010

By Matthew

Matthew M. Linton
mlinton@kcfpc.com

John R. Mann
jmann@kcfpc.com

KENNEDY CHILDS & FOGG, P.C.
633 17th Street, Suite 2200
Denver, Colorado 80265
PHONE: (303) 825-2700
FAX: (303) 825-0434

LOCAL COUNSEL FOR *AMICI CURIAE*

Kevin S. Bankston (*application for admission forthcoming*)

bankston@eff.org

Jennifer Granick (*application for admission forthcoming*)

jennifer@eff.org

ELECTRONIC FRONTIER
FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
PHONE: (415) 436-9333
FAX: (415) 436-9993

ATTORNEYS FOR *AMICI CURIAE*

Paul Ohm (*application for admission forthcoming*)

paul.ohm@colorado.edu

SAMUELSON-GLUSHKO
TECHNOLOGY LAW & POLICY
CLINIC

University of Colorado Law School
401 UCB
Boulder, CO 80309
PHONE: (303) 492-0384
FAX: (303) 492-1200

ATTORNEY FOR *AMICI CURIAE*

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

IN RE APPLICATION OF THE
UNITED STATES OF AMERICA
FOR AN ORDER PURSUANT TO
18 U.S.C. § 2703(d)

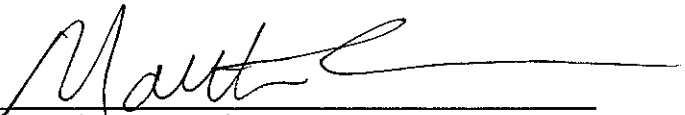
Misc. No. 09-Y-080 CBS

***AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION,
THE CENTER FOR DEMOCRACY & TECHNOLOGY, THE
CENTER FOR FINANCIAL PRIVACY AND HUMAN RIGHTS,
THE COMPETITIVE ENTERPRISE INSTITUTE, THE
COMPUTER & COMMUNICATIONS INDUSTRY
ASSOCIATION, THE DISTRIBUTED COMPUTING INDUSTRY
ASSOCIATION, GOOGLE, INC., NETCOALITION, THE
PROGRESS & FREEDOM FOUNDATION AND TRUSTE
CORPORATE DISCLOSURE STATEMENT**

Amici Electronic Frontier Foundation, The Center For Democracy & Technology, The Center For Financial Privacy And Human Rights, The Competitive Enterprise Institute, The Computer & Communications Industry Association, The Distributed Computing Industry Association, Google Inc., Netcoalition, The Progress & Freedom Foundation And TRUSTe by and through their local counsel and pursuant to FED. R. CIV. P. 7.1 and D.C.COLO. L. CIV. R. 7.4, hereby files this Corporate Disclosure Statement, and states as follows:

None of the *amici* have a parent corporation, and no publicly traded corporation currently owns more than 10% of any *amici*'s stock.

DATED: April 13, 2010

By 

Matthew M. Linton
mlinton@kcfpc.com

John R. Mann
jmann@kcfpc.com

KENNEDY CHILDS & FOGG, P.C.

633 17th Street, Suite 2200

Denver, Colorado 80265

PHONE: (303) 825-2700

FAX: (303) 825-0434

LOCAL COUNSEL FOR *AMICI CURIAE*

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

IN RE APPLICATION OF THE
UNITED STATES OF AMERICA
FOR AN ORDER PURSUANT TO
18 U.S.C. § 2703(d)

Misc. No. 09-Y-080 CBS

**CERTIFICATE OF SERVICE BY *AMICI CURIAE*
ELECTRONIC FRONTIER FOUNDATION, THE CENTER FOR
DEMOCRACY & TECHNOLOGY, THE CENTER FOR
FINANCIAL PRIVACY AND HUMAN RIGHTS, THE
COMPETITIVE ENTERPRISE INSTITUTE, THE COMPUTER
& COMMUNICATIONS INDUSTRY ASSOCIATION, THE
DISTRIBUTED COMPUTING INDUSTRY ASSOCIATION,
GOOGLE INC., NETCOALITION, THE PROGRESS &
FREEDOM FOUNDATION AND TRUSTE RE: THE UNITED
STATES' MOTION TO COMPEL COMPLIANCE WITH THIS
COURT'S 2703(d) ORDER**

The undersigned hereby certifies that on this 13th day of April, 2010,

I deposited in United States Mail the following documents:

- MOTION OF ELECTRONIC FRONTIER FOUNDATION, *ET AL.* FOR LEAVE TO FILE BRIEF AS *AMICI CURIAE* OPPOSING THE UNITED STATES' MOTION TO COMPEL COMPLIANCE WITH THIS COURT'S 2703(d) ORDER
- BRIEF OF *AMICI CURIAE* OPPOSING THE UNITED STATES' MOTION TO COMPEL COMPLIANCE WITH THIS COURT'S 2703(d) ORDER
- *AMICI CURIAE* CORPORATE DISCLOSURE STATEMENT

to the addresses of counsel for the interested parties as set forth below. I

also sent courtesy copies by email to the email addresses indicated below.

Attorneys for Yahoo!:

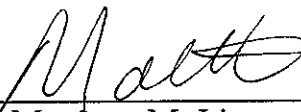
Marc J. Zwillinger
Zwillinger Genetski LLP
1705 N. Street, NW
Washington, D.C. 20036
marc@zwillgen.com
(202) 706-5202 (direct)
(202) 296-3585 (main office)

Attorneys for the United States:

David M Gaouette
Pegeen D. Rhyne
United States Attorney's Office
1225 17th Street, Suite 700
Denver, Colorado 80202
Pegeen.Rhyne@usdoj.gov
(303) 454-0100
(303) 454-0409 (fax)

DATED: April 13, 2010

By



Matthew M. Linton
mlinton@kcfpc.com

John R. Mann
jmann@kcfpc.com

KENNEDY CHILDS & FOGG, P.C.

633 17th Street, Suite 2200

Denver, Colorado 80265

PHONE: (303) 825-2700

FAX: (303) 825-0434

LOCAL COUNSEL FOR *AMICI CURIAE*