No. 06-4092

IN THE UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

STEVEN WARSHAK,

Plaintiff-Appellee,

v.

UNITED STATES OF AMERICA,

Defendant-Appellant.

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

BRIEF FOR PROFESSORS OF ELECTRONIC PRIVACY LAW AND INTERNET LAW AS *AMICI CURIAE* SUPPORTING THE APPELLEE AND URGING AFFIRMANCE

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

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

(affiliations for identification purposes only)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Cases

Other Authorities

INTEREST OF AMICI

Amici are scholars who teach, write about, or have an interest in electronic privacy law and Internet law. Amici have no stake in the outcome of this case, but are interested in ensuring that electronic privacy law develops with due regard for the vital role electronic communications play in our lives. A full list of amici is appended to the signature page. Both defendant-appellant and plaintiff-appellee have consented to the filing of this brief.

SUMMARY OF ARGUMENT

Electronic mail ("e-mail') has become an essential medium of communication and assumed a vital role in our lives. The contents of our e-mail accounts reveal extensive and detailed information about our interests, our views, and our actions. Yet, the Government in this case claims the right to obtain the entirety of our personal e-mail accounts from our service providers, without first establishing probable cause or providing us notice, so long as we have previously accessed our e-mails in some way. Acceptance of this radical claim would dramatically limit judicial oversight of an immensely powerful surveillance tool and eviscerate the privacy of electronic communications.

Though the Government presents the question as well settled, no federal courts have addressed government acquisition of e-mail from a service provider without prior notice ("stored e-mail surveillance"), although two military courts

have found that it requires a probable cause warrant.[1] More fundamentally, when the Government argues that a constitutional "reasonableness" standard applies to stored e-mail surveillance because the applicable statute apparently approves of subpoena-like authority, it begs the essential question: does stored e-mail surveillance by the Government on less than probable cause satisfy the Fourth Amendment? Amici, law professors who write and teach in the areas of electronic privacy law and Internet law, believe that it does not.

Because it invades a reasonable expectation of privacy, stored e-mail surveillance constitutes a search under the Fourth Amendment, and may not be conducted without first obtaining a warrant based on probable cause. "Compelling" a service provider to produce a person's e-mail does not entitle government agents to evade that constitutional requirement.

ARGUMENT

I. STORED E-MAIL SURVEILLANCE IS A SEARCH UNDER THE FOURTH AMENDMENT THAT REQUIRES, AT A MINIMUM, A WARRANT BASED ON PROBABLE CAUSE

Courts, and not Congress, must determine the threshold issue: how does the Constitution regulate stored e-mail surveillance? Because government agents intrude upon users' reasonable expectation of privacy when they acquire private e-

[1] Amici do not address what procedural requirements apply when the government does give the target prior notice.

mails, they conduct a search under the Fourth Amendment.[2] That expectation of privacy obtains whether the e-mails acquired are stored or in transit, and whether or not their recipients have accessed them. Nothing in the private contracts between users and their internet service providers affects the application of those constitutional protections.

A. Users Maintain a Reasonable Expectation of Privacy in Their E-mails, Whether or Not Those E-mails Have Been Stored or Accessed.

Users maintain a reasonable expectation of privacy in their e-mail, whether that e-mail is in transit or has come to rest. *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). The reasonable expectation of privacy test, which is used to determine whether a particular investigatory technique constitutes a search under the Fourth Amendment, asks whether target of an investigation entertains an actual expectation of privacy in the object of the search (subjective prong), and whether that expectation of privacy is one that society deems reasonable (objective prong). *See Kyllo v. United States*, 533 U.S. 27, 32-33 (2001); *Katz v. United States*, 389 U.S. 347, 361 (1967).

[2] The First Amendment also supports imposing significant burdens on law enforcement access to e-mails, because they are communications. *See, e.g., Stanley v. Georgia*, 394 U.S. 557, 564 (1969) ("It is now well established that the Constitution protects the right to receive information and ideas."); *see also* Daniel Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. (forthcoming 2007).

1. Warshak had a subjective expectation of privacy in the e-mails stored with his service providers.

Warshak's use of his e-mail demonstrates his subjective expectation of privacy in it. *See* Plaintiff-Appellee Warshak's Opposition to United States' Motion To Stay Preliminary Injunction, No. 06-4092, at 11 n.6 (6th Cir. filed Nov. 2, 2006) ("Warshak Stay Opposition"). The subjective prong precludes affording constitutional protection to those who themselves did not view the object of the investigation as private. To require that government agents refrain from viewing information easily seen by others is unfair and unnecessary. It is unfair because the government should not be disadvantaged vis-à-vis the average member of the public. It is unnecessary because we assume that before people make information available to all they have either determined the repercussions to be harmless, or assumed the risk of those repercussions. The Constitution does not protect information that one has "knowingly expose[d] to the public," *Katz*, 389 U.S. at 351.

In this case, there is no evidence that Warshak knowingly exposed the entirety of his e-mail accounts to the public. Instead, Warshak used the e-mail accounts the government seized to send e-mails "of a deeply personal nature." *See* Warshak Stay Opposition at 4 n.1. As we discuss in Part I.B below, that Warshak maintained e-mail accounts with service providers did not vitiate his subjective expectation of privacy.

2. Warshak's expectation of privacy in his e-mails was objectively reasonable.

E-mail has become so indispensable that it must be reasonable for us to expect that it is private. One who looks at our e-mails obtains a detailed view into our innermost thoughts; no previous mode of surveillance exposes more. When we compose private and professional e-mails, embed links to Internet sites in some, and attach documents, pictures, sound files and videos to others, we rely on the privacy of the medium. Society does not make us rely at our peril but rather accepts as reasonable our expectations of privacy in e-mail.

The public reasonably expects e-mail to be private, despite the fact that e-mail may be vulnerable to surveillance. The Supreme Court found the expectation of privacy in telephone calls to be reasonable in *Katz*, despite public awareness of the vulnerability of those calls to interception. In the years preceding *Katz*, the public had learned of rampant illegal wiretapping from numerous influential books, scholarly articles, and newspaper accounts. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act,* 56 ALA. L. REV. 9, 38-39 (2004). In the same period, Congress considered new legislation and convened numerous hearings and commissioned lengthy expert reports that detailed communications' vulnerability. *Id*. at 74-75. The *Katz* Court nonetheless found warrantless wiretapping to be unconstitutional, despite the lack of absolute privacy in telephone calls. *See id*. at 38. Similarly, a government pronouncement that e-

mails are vulnerable may not defeat our reasonable expectations of privacy in it. *See Smith v. Maryland*, 442 U.S. 735, 740 n.5 (1979) (recognizing that the expectation of privacy analysis must be replaced by a normative analysis when "subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms.") Otherwise, the Constitution would be powerless to prevent executive branch overreaching.

In *Katz,* the Supreme Court based constitutional protection of telephone calls on the overriding importance of the telephone system. *Katz*, 389 U.S. 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 other words, whatever people actually thought or knew about the privacy of their telephone calls, they were *entitled to believe* in the privacy of telephone calls, because any other result would be destructive of society's ability to communicate. *Id*. (holding that one who places a telephone "call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

Because e-mails typically contain much richer data than telephone calls, e-mail surveillance intrudes much more on personal privacy than does an analogous wiretap. Although many modern e-mails incorporate other media, even a simple text e-mail can reveal a lengthy back-and-forth exchange between the parties to the correspondence. People reveal in their e-mails much more about their political

opinions, religious beliefs, personal relationships, intellectual interests, and artistic endeavors than they ever revealed over the telephone. Stored e-mails, in particular, contain a vast archive of people's past activities.

Society now relies on e-mail and its powerful features much more than it relied on the telephone system at the time of *Katz*. Because of e-mail's vital role in modern communications, users have a reasonable expectation of privacy it, and agents must secure at least a probable-cause warrant under the Fourth Amendment before they obtain it.[3]

3. Warshak had a reasonable expectation of privacy in his e-mails after his service provider stored them and he accessed them.

Stored e-mail should not receive less constitutional protection than e-mail in transit. *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). More extensive e-mail correspondence may be found on a third party's server than may be intercepted. When a government agent intercepts e-mails in transit, she acquires only the e-mail

[3] Several Courts of Appeals imposed the heightened procedural requirements for wiretapping on silent video surveillance because it was just as intrusive, continuous, hidden and indiscriminate. *See, e.g.***,** *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir.) (en banc), *cert. denied*, 506 U.S. 1005 (1992) (imposing the following constitutional requirements in addition to probable cause: particular description, last resort, limited time, and minimization). Because e-mail surveillance threatens privacy and risks abuse as much as wiretapping, it too should be subject to the heightened requirements. *See* Freiwald, *Online Surveillance*.

traveling at that moment. The agent must continue the surveillance for so long as she hopes to track the target's correspondence. To obtain e-mails covering a vast length of time, it would be far simpler and easier to conduct stored e-mail surveillance afterwards in a single shot. For example, rather than running an e-mail wiretap for three months from January 1 to March 31, an agent may obtain the same electronic communications from the service provider by demanding, on March 31, prior e-mails going back three months. That the government apparently obtained thousands of e-mails, both sent and received, from Warshak's service providers, from accounts over nine years old, starkly illustrates the power and scope of stored e-mail surveillance. *See* Warshak Stay Opposition at 2, 11.

By the same token, a user should enjoy full Fourth Amendment protection for e-mail messages that she has accessed.[4] Nothing in the reading of an e-mail (let alone its being opened) makes the correspondence less private or its acquisition less intrusive. Users leave copies of their already-read e-mails in their accounts for many reasons, and almost never out of a lack of concern for the privacy of those e-mails. In fact, most users delete their least important, least sensitive e-mails, and retain the others for later use. Users store private e-mails in their accounts because they do not know how to do otherwise, or because they are not aware that their

[4] Amici use the term "accessed" to cover accessed, opened, viewed, and downloaded e-mail. The Government claims the right to acquire accessed e-mails, draft e-mails and sent e-mails without a probable cause warrant.

service providers maintain copies.[5] Many users simply neglect to delete e-mails until they run out of storage space; that retention does not indicate that users have knowingly exposed those e-mails to public or law enforcement view. The government's strained statutory argument should not confuse the fact that a user's access to his e-mail does not affect its constitutional protection.

Before obtaining disclosure of the contents of an e-mail account stored on a service provider's computer, the Fourth Amendment requires that government agents obtain, at a minimum, a probable cause warrant, or that they invoke a proper exception to the warrant requirement. "The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." *United States v. United States Dist. Ct.*, 407 U.S. 297, 317 (1972). That stored e-mail surveillance takes place entirely outside of the reach and knowledge of the target makes it particularly prone to abuse. The warrant requirement protects e-mails whether in transit or stored, and whether accessed or not.[6]

---

[5] Service providers may retain e-mails as a matter of practice or government compulsion. See 18 U.S.C. § 2704 (compelling backup preservation of electronic communications).

[6] As discussed, a probable cause warrant alone may be constitutionally insufficient. *Supra* note 3.

B. E-mail Users Do Not Forfeit an Expectation of Privacy in their Communications Merely by Storing Those Communications with a Service Provider, Even Where the Service Provider Retains a Right of Access.

The Government's argument that an e-mail user forfeits any expectation of privacy and exposes her e-mail to indiscriminate government surveillance when she relies on a service provider to transmit and store that e-mail ignores a range of cases in which courts have recognized an expectation of privacy in items held by a third party. Moreover, it misunderstands the significance to this dispute of the Stored Communications Act[7] and of service providers' policies and practices regarding access to the communications they store.

1. Allowing a third party to carry or store an item does not eliminate any expectation of privacy in that item.[8]

Placing something in the care of a third party does not, without more, make the government free to acquire it without a warrant. The Government's argument to the contrary appears to stem from a broad reading of the Supreme Court's "business records" cases. *See* Brief for the United States, Warshak v. United States, No. 06-4092, at 36-40, 43-45 (6th Cir. filed Oct. 11, 2006) ("Government Brief"). The post–*Katz v. United States* foundation for this line of cases is *United*

[7] 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.A. § 2701 *et seq.*).

[8] Portions of this discussion are drawn from Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1397-1413 (2004).

States v. Miller, 425 U.S. 435 (1976),[9] where the Supreme Court held that a bank customer had no reasonable expectation of privacy in financial records held by his banks, because "[a] depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *Id.* at 443; *see also Smith v. Maryland*, 442 U.S. 735 (1979) (holding that user has no expectation of privacy in telephone numbers revealed to the telephone company to connect calls).

Miller and its progeny do not support the Government's position that communications placed in the hands of a third party are subject to compelled disclosure merely because a third party holds them. *Miller* relied on two lines of cases to arrive at the assumption-of-risk language quoted above. First, *Miller* relied on pre-*Katz* cases evaluating the compelled disclosure of business records under a reasonableness standard. The Court confirmed the post-*Katz* vitality of the reasonableness analysis by concluding that financial records that form part of a business relationship with the bank are not the kind of items in which one can expect privacy. *See Miller*, 425 U.S. at 440-42. Second, *Miller* drew upon a

[9] In a prior case, *Couch v. United States*, 409 U.S. 322 (1973), the Court addressed a Fourth Amendment challenge to an IRS summons compelling an accountant to surrender records used in preparing the defendant's tax return. The Court gave the Fourth Amendment claim only brief treatment because it "[did] not appear to be independent of [the taxpayer's] Fifth Amendment argument." 409 U.S. at 325-26 n.6. The Court's reasoning was similar to that which it later employed in *Miller*. *See id.* at 336 n.19.

series of cases involving communications revealed, recorded, or transmitted to the government by an informant or undercover agent who is a party to the communication. *See Miller*, 425 U.S. at 443. In those cases, the Court had reasoned that "no interest legitimately protected by the Fourth Amendment is involved," because the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." *Hoffa v. United States*, 385 U.S. 293, 302 (1966); *see also United States v. White*, 401 U.S. 745, 749, 751 (1971) (plurality opinion); *Osborn v. United States*, 385 U.S. 323, 331 (1966); *Lopez v. United States*, 373 U.S. 427 (1963).

Neither of the two lines of cases on which *Miller* relies points toward the Government's categorical rule that one loses one's expectation of privacy by allowing a provider to transmit or store communications. Communications are not business records of the sort contemplated in *Miller* and its progeny. And to place a communication in the hands of a third party for carriage or storage is not to "confide" or "reveal" that communication in the same sense that one "confides" or "reveals" something to a government informant or agent by speaking to that person, or in the sense that a depositor "reveals" something to a bank so that the bank can process a transaction, or in the sense that one "reveals" a telephone number so that the telephone company can connect a call. Indeed, any categorical

rule that a provider's involvement eliminates a user's reasonable expectation of privacy runs headlong into the Court's holding in *Katz v. United States. Katz*, after all, involved communications carried over a telephone line by a communications carrier that undoubtedly had the technical ability to monitor the communications. 389 U.S. 347, 353 (1967). If the Government's reasoning in this case were correct, *Miller* would have overruled *Katz sub silentio*, even while the *Miller* Court purported to affirm and apply *Katz*.

Moreover, in a range of contexts, courts have recognized that a third-party's involvement in carrying or storing property does not leave government agents free to inspect that property. When the U.S. Postal Service carries mail or a sealed package, for example, government agents cannot open the items without obtaining a warrant. As the Supreme Court has recognized, "[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable." *United States v. Jacobsen*, 466 U.S. 109, 114 (1984); see also *Ex parte Jackson*, 96 U.S. 727, 733 (1877) ("Letters and sealed packages . . . are as fully guarded from examination and inspection . . . as if they were retained by the parties forwarding them in their own domiciles.").

Similarly, when someone maintains personal property on a third party's premises, she retains an expectation of privacy in it, so long as the property is

secured against others' access and the third party's right of access to the premises is limited. *See, e.g.*, *Stoner v. California*, 376 U.S. 483, 489 (1964) (search of hotel room without warrant violated Fourth Amendment, even though one who engages a hotel room gives implied permission to hotel personnel to enter to perform their duties); *Chapman v. United States*, 365 U.S. 610, 616-18 (1961) (search of house occupied by tenant violated Fourth Amendment, even though landlord had authority to enter house for some purposes); *United States v. Johns*, 851 F.2d 1131, 1133-35 (9th Cir. 1988) (implicitly recognizing reasonable expectation of privacy in rented storage unit); *cf. United States v. Rahme*, 813 F.2d 31, 34 (2d Cir. 1987) (where hotel guest failed to pay rent and rental period expired, hotel could lawfully take possession of items in room and guest had no reasonable expectation of privacy); *United States v. Poulsen*, 41 F.3d 1330, 1336 (9th Cir. 1994) (renter of storage unit loses expectation of privacy when he fails to pay rent, and facility manager may seize property and turn it over to law enforcement).

This case is analogous to cases involving a third party's carriage or storage of physical property. Agents here sought to remove e-mail communications from a storage area set aside exclusively for the use of the subscriber and to which nobody but the provider had physical access. Yet the Government does not cite or discuss

these cases. Instead, it seeks a categorical rule that third-party involvement extinguishes an expectation of privacy.

2. Service provider assistance to government agents does not reduce the government's constitutional obligations.

The Government builds much of its case on the fact that its agents obtained Warshak's stored e-mail from his service providers. But the Government may not avoid its constitutional obligations by an engaging an intermediary in its surveillance. The Government also argues that service providers' technical ability to access and scan communications for harmful content and attachments, or terms of service announcing that it may do so, can eliminate users' expectation of privacy in communications stored with such providers. Government Brief at 49. Crediting that claim would misconstrue the applicable statute, the nature of a service provider's right to protect its own property, and the nature of the contractual relationship between users and their service providers.

a. The involvement of a service provider in the Government's stored e-mail surveillance does not impact the Government's constitutional obligations.

A service provider acts as the government's agent when it accedes to surveillance requests. *See United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006) (describing seizure of stored e-mail by network administrator as "a part of a search for law enforcement purposes"). When the Government initiates the search of the

target's email account, as it did in this case, the service provider's actions to facilitate the search do not convert the Government's surveillance from state action subject to Fourth Amendment requirements to a private search. *See United States v. Maxwell*, 45 M.J. 406, 422 (C.A.A.F. 2006) (service provider's search of stored e-mail at government's request not a "private search"); *see also McClelland v. McGrath*, 31 F. Supp. 2d 616, 619 (N.D. Ill. 1998) (noting that when telephone company employees act "at the request or direction of police officers," they act as government agents and the Fourth Amendment applies).

In addition, when electronic communications providers furnish stored e-mail to government investigators, that parallels the common practice of telecommunications companies providing telephone line access to government wiretappers. Wiretapping assistance is not only statutorily mandated,[10] it has never reduced the government's constitutional obligations.[11] Service provider involvement in stored e-mail surveillance does not reduce the constitutional regulation of that practice either.

[10] *See* 18 U.S.C. § 2518(4) (requiring and regulating provider assistance).

[11] Service provider assistance in government surveillance does impose statutory obligations on the service provider in addition to any constitutional ones. *See* 18 U.S.C. § 2707 (permitting civil suits against service providers for improper disclosure).

b. Terms of service providing that the government may be granted access do not affect the constitutional requirements for stored e-mail surveillance.

The Government argues that most service providers have policies stating that they will disclose communications in response to legal process, and that this fact eliminates any expectation of privacy in e-mail communications. *See* Government Brief at 34. A service provider's policy of complying with legal process, however, cannot defeat a user's reasonable expectation of privacy. E-mail users must be entitled to presume that agents will present *appropriate* legal process, not that they will present *any* legal process. It would turn the law on its head if service providers could merely notify their users that they intend to comply with unconstitutional government demands and thereby immunize the government from constitutional claims.

c. The fact that service providers can and do screen e-mail under certain circumstances does not eliminate a user's expectation of privacy vis-à-vis government agents.

The Government errs when it claims that Congress, through adoption of the Stored Communications Act ("SCA"), granted service providers an unfettered right to access users' e-mail and thereby extinguished any expectation of privacy. Congress simply cannot extinguish a constitutional right by statute. Moreover, the SCA grants no such unfettered right of access. It is true that a service provider is not subject to *federal criminal prosecution and civil liability* under the SCA for

unauthorized access of its subscribers' communications. Contrary to the Government's suggestion, however, immunity from criminal or civil liability under one particular federal statute is not the same thing as an unfettered right of access, for it says nothing about other sources of law (including other federal statutes, contractual provisions, state statutes, or common law protections) that might limit a service provider's access to a user's communications. *See United States v. Councilman* 418 F.3d 67, 82 (1st Cir. 2005) (en banc) (declining to dismiss federal Wiretap Act charge against service provider despite absence of SCA liability).

If communications providers retain broad rights of access to user e-mails in their own terms of service, those provisions do not concern the relationship between the user and the government. Terms of service set forth the ways in which a service provider may need to protect its system and business from fraud, hacking, unauthorized use, and the like. Whatever rights the service provider might have to access communications to perform those functions, those rights do not give the service provider the right to disclose communications for the fundamentally different purpose of assisting law enforcement investigations of unrelated crimes. *United States v. Long*, 64 M.J. 57, 63 (C.A.A.F. 2006) (consent to monitoring did not imply consent to "engage in law enforcement intrusions by

examining the contents of particular e-mails in a manner unrelated to maintenance of the e-mail system.").[12]

Notwithstanding its terms of service, a service provider's right to protect its own property does not release the Government from the constraints of the Constitution. Any third party that holds property on behalf of another, such as a storage company, may retain the right to inspect units to prevent damage that might occur to its property or that of other customers. The fact that the storage company has or exercises such a right, however, says nothing about the relationship between the storage customer and government agents. A storage company may, on its own initiative and independently of government action, provide to the Government the fruits of its own inspection. But that does not give government agents license to conduct their own warrantless search of a storage unit or to demand that the storage company search it on the Government's behalf. When the Government or its agent examines the contents of the storage locker, it invades a reasonable expectation of privacy, even though the storage company retained some right of access to protect its property.

[12] Whether a user forfeits an expectation of privacy when he violates those terms of service, is not at issue in this case. *See United States v. Young*, 350 F.3d 1302, 1308 (11th Cir. 2004) (expectation of privacy in package unreasonable when user shipped large amounts of cash in violation of clear carrier contract after acknowledging carrier's unqualified right to inspect).

In short, Warshak retained an expectation of privacy in his e-mails stored on his service providers' systems, notwithstanding their involvement in the search, their contract with him, or their business practices. As a result, the government needed to obtain at least a probable-cause warrant before conducting the stored e-mail surveillance in this case.

II. GOVERNMENT AGENTS CANNOT EVADE THE FOURTH AMENDMENT'S WARRANT REQUIREMENT BY COMPELLING PRODUCTION OF COMMUNICATIONS FROM THIRD-PARTY SERVICE PROVIDERS

For access to communications subject to a reasonable expectation of privacy, such as stored e-mails, the Fourth Amendment requires that government agents obtain (at a minimum) a warrant based on probable cause. Nevertheless, the Government argues that its agents need only satisfy a "reasonableness" standard when they "compel production" of materials. Government Brief at 36. To be clear, the Government does not argue merely that a reasonableness standard applies *when the target lacks a reasonable expectation of privacy* in the items the agents seek. Rather, the Government argues that the reasonableness standard applies *even when the target has a reasonable expectation of privacy*. *See id.* at 38 (arguing that "a target's reasonable expectation of privacy affects only his standing to challenge the reasonableness of compelled disclosure"). This argument cannot withstand scrutiny. Government agents simply cannot write the warrant

requirement out of the Fourth Amendment by compelling production of evidence whenever they wish, without regard for the underlying constitutionally-protected privacy interests.

The Government's error stems from an over-reading of cases applying a "reasonableness" standard where government agents have used a subpoena to compel production of documents or other items. Properly understood, those cases identify two overlapping circumstances in which a reasonableness standard may be appropriate: (1) where the target of an investigation has no reasonable expectation of privacy in the items the agents seek; and (2) when an agency uses a statutorily authorized administrative subpoena in aid of its regulatory mission, and pre-enforcement judicial process is available to evaluate the intrusiveness of its demands. Neither circumstance is present here.

A. Use of a "Reasonableness" Test to Evaluate Compelled Production of Evidence Ordinarily Presumes or Follows a Determination that the Target of the Investigation Lacks a Reasonable Expectation of Privacy in the Items Agents Seek.

In arguing that there is a well established body of law applying a "reasonableness" standard to evaluate compelled production of materials, Government Brief at 38-39, the Government ignores a key unifying theme of this case law: that the use of a reasonable subpoena to compel production of materials is permissible where the target of the investigation *lacks any expectation of privacy* in those materials.

In its effort to draw a categorical distinction between searching for evidence and compelling its production, the Government relies on language in *United States v. Dionisio*, 410 U.S. 1 (1973), a case involving whether a subpoena compelling individuals to appear before a grand jury and to give voice exemplars violated the Fourth Amendment. *Id.* at 3; *see* Government Brief at 39. *Dionisio* in fact undermines the Government's position, for it illustrates that use of a subpoena does not eliminate the need to inquire into a target's expectation of privacy. The Court bifurcated its analysis of the respondents' Fourth Amendment challenge, first concluding that the *order that the individuals appear* before the grand jury did not constitute an unlawful seizure, *Dionisio*, 410 U.S. at 9-10, and then examining whether, once the individuals were lawfully before the grand jury, the further *direction to make voice recordings* constituted an unlawful search, *id.* at 13-15. The language on which the Government relies addressed only the first question, concerning the distinction between an arrest and a subpoena compelling one's appearance. On the second question, the Court concluded that no reasonable expectation of privacy existed, since the Fourth Amendment does not protect physical characteristics, such as the sound of one's voice, that an individual knowingly and necessarily exposes to the public. *Id.* at 14. What matters here is the Court's mode of analysis: The Court did not suggest that the mere use of a subpoena eliminates any need to inquire into any expectation of privacy. Rather, it

recognized that compelled production of evidence can be sufficiently intrusive and immediate to constitute a search. Its assessment of whether the respondents had a reasonable expectation of privacy in voice characteristics would have been unnecessary if the Government's theory in this case were correct.

The "business records" cases on which the Government relies—in which courts applied a reasonableness standard in evaluating the use of subpoenas to compel production of corporate books and documents—carry similar import. *See* Government Brief at 36-40, 43-45. Many of those cases predated the Court's decision in *Katz v. United States*, *see* Government Brief at 36 (referring to "[a] century of Supreme Court case law"); *id.* at 38-89 (citing *Wilson v. United States*, 221 U.S. 361 (1911); *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186 (1946)), and thus have no bearing on whether use of a subpoena categorically defeats a reasonable expectation of privacy. In rejecting Fourth Amendment claims in such cases, the Court consistently underscored the fact that the records involved were merely corporate records. *See Walling*, 327 U.S. at 208 (distilling prior case law as follows: "[I]n so far as [earlier cases] apply merely to the production of corporate records and papers in response to a subpoena or order authorized by law and safeguarded by judicial sanction," those cases establish that the Fourth Amendment "guards against abuse only by way of too much

indefiniteness or breadth . . . if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant.").

The Court's decision in *Katz* spurred new challenges to agents' acquisition of corporate records, on the theory that the owner or subject of the records had a reasonable expectation of privacy in the documents. The Supreme Court first squarely addressed such a claim in *United States v. Miller*, 425 U.S. 435 (1976), discussed above. *See supra* pp. 10-13. The Court concluded that the target of the investigation lacked any expectation of privacy in the documents and upheld the compelled disclosure, the reasonableness of which was uncontested by the banks to whom the subpoenas were issued. *See Miller*, 425 U.S. at 446 n.9. Importantly, the Court never suggested that an inquiry into Miller's reasonable expectation of privacy was unnecessary because government agents proceeded by subpoena; it said that no expectation of privacy existed. Although *Miller* establishes the post-*Katz* vitality of a "reasonableness" analysis in cases involving compelled disclosure of business records, it is important to understand *why* a reasonableness analysis applies in *Miller* and subsequent cases. It is not because a target's expectation of privacy can always be overcome by a mere subpoena. Rather, it is because the targeted materials in cases such as *Miller* involve no expectation of privacy. Indeed, as the Court has observed, "[s]pecial problems of privacy" may be presented by attempts to compel production of items that are not business

records, such as a personal diary. *Fisher v. United States*, 425 U.S. 392, 401 n.7 (1976).

The subpoena cases on which the Government relies to suggest that use of a subpoena categorically eliminates the need to inquire into the target's expectation of privacy are additional cases in the *Miller* line. *See, e.g.*, *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984) (seeking payroll and sales records, which the Court characterized as "corporate books or records"); *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (seeking financial records).

The Government cites only a single post-*Katz* case in which a court sustained the use of a subpoena to compel production of property despite the court's explicit assumption that the target of the investigation maintained an expectation of privacy in the property sought. In *United States v. Palmer*, 536 F.2d 1278 (9th Cir. 1976), the Court of Appeals for the Ninth Circuit held that the government did not violate the Fourth Amendment when it compelled a defendant's attorney to produce property held on the defendant's behalf. The court reasoned that "a properly limited subpoena does not constitute an unreasonable search and seizure under the fourth amendment." *Id.* at 1282.

In reaching this conclusion, *Palmer* relied on business cases pre-dating *Miller*, including *Walling*, *Hale v. Henkel*, 201 U.S. 43, 70 (1906) and others. *Palmer* was decided within six weeks of *Miller* and did not cite that decision.

Because *Palmer* relied exclusively on cases that the *Miller* Court clarified involved no reasonable expectation of privacy, it is not persuasive authority for the proposition that a subpoena is appropriate even where a reasonable expectation of privacy exists.

B. Administrative Subpoena Cases Are Wholly Inapplicable in This Case.

The Government also relies on administrative subpoena cases to support a categorical distinction between compelling production of evidence and searching for evidence. *See* Government Brief at 40-41 (citing *In re Administrative Subpoena John Doe, D.P.M.*, 253 F.3d 256 (6th Cir. 2001); *United States v. Morton Salt Co.*, 338 U.S. 632 (1990)); *id.* at 39 (citing *In re Subpoena Duces Tecum (United States v. Bailey)*, 228 F.3d 341 (4th Cir. 2000)). The rationale for evaluating an administrative subpoena under a reasonableness inquiry does not apply in this case.

Case law concerning administrative subpoenas recognizes that, when a corporation's activities affect interstate commerce, the federal Government has an investigative power analogous to the "visitorial" power of the incorporating state. *See Oklahoma Press Pub'g Co. v. Walling*, 327 U.S. 186, 204 (1946). Accordingly, Congress may grant an agency a "power of inquisition" into whether the law that the agency administers is being violated, *see Morton Salt*, 338 U.S. at 642; *id.* at 652 (noting that "the privilege of engaging in interstate commerce"

carries with it "an enhanced measure of regulation"), and courts will test the use of such a subpoena under a reasonableness analysis, *see In re Administrative Subpoena John Doe, D.P.M.*, 253 F.3d 256, 265 (6th Cir. 2001).

Although the Government contends that the § 2703(d) orders at issue in this case are analogous to administrative subpoenas, *see* Government Brief at 41 n.7 (characterizing § 2703(d) orders as "a form of agency investigative authority" analogous to that recognized in *Morton Salt*), they are not. Even those statutes authorizing the Attorney General to issue administrative subpoenas as a prelude to a criminal investigation specify the narrow regulatory function the subpoena authority must serve. *See, e.g.*, 21 U.S.C. § 876 (2000) (authorizing use of administrative subpoenas in investigations "relating to the [Attorney General's] functions under this subchapter with respect to controlled substances, listed chemicals, tableting machines, or encapsulating machines"); 18 U.S.C. § 1968 (2000) (authorizing a "civil investigative demand" for "documentary materials relevant to a racketeering investigation"); 18 U.S.C. § 3486(a)(1)(A)(i) (2000) (authorizing administrative subpoenas in connection with investigation of health care offenses or sexual exploitation or abuse of children). In contrast, § 2703 is a general rule of criminal procedure, analogous to Rule 41 of the Federal Rules of Criminal Procedure and untethered to any specific regulatory function. Cases concerning administrative subpoenas are thus wholly inapplicable in this case.

Even if administrative subpoena cases were relevant here, those cases do not support the Government's position that an inquiry into a reasonable expectation of privacy is irrelevant whenever government agents choose to compel production of rather than search for evidence. Administrative subpoena cases recognize not only that such subpoenas must serve a narrow regulatory mission, but also that the legitimacy of an administrative subpoena derives from the judicial process available to test the intrusiveness of the subpoena before it is enforced. Two of the administrative subpoena cases on which the Government relies—both dealing with administrative subpoenas in connection with health care fraud investigations—illustrate this principle. In *In re Subpoena Duces Tecum (United States v. Bailey)*, 228 F.3d 341, 348 (4th Cir. 2000), the Court of Appeals for the Fourth Circuit explained that a subpoena "commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands. . . . As judicial process is afforded *before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from*, that process." (Emphasis added.) Similarly, in *In re Administrative Subpoena John Doe, D.P.M.*, 253 F.3d 256, 264 (6th Cir. 2001), this Court recognized that the target of the administrative subpoena had an opportunity to challenge the intrusiveness of that subpoena before complying with it. In both of these cases, the target of the subpoena was also the target of the investigation, and thus could assert any

relevant privacy interests in the documents requested before a court enforced the subpoena.

An order to compel production of e-mail is distinct from the administrative subpoenas used in *Bailey* and *Doe* in two obvious respects. First, because the service provider on whom a § 2703(d) order is served is not the target of the investigation, and only the recipient of the order has an opportunity to challenge it, the target of the investigation has no opportunity parallel to that of Bailey or Doe to assert that the order is unduly intrusive. To be sure, as the Government notes, the Supreme Court has applied a reasonableness test to evaluate subpoenas even when agents compel disclosure of information held by parties who are not themselves the subject of an investigation. *See* Government Brief at 43. As discussed above, however, the evaluation of a third-party subpoena under a reasonableness standard either presumes or follows a prior determination that the target of the investigation lacks an expectation of privacy in the items compelled. *See supra* pp 21-26.

Second, in both *Bailey* and *Doe*, the documents the agents sought were records compiled in the ordinary course of a business relationship—records in which (as explained above) the Supreme Court has found any expectation of privacy to be unreasonable. *See supra* pp. 10-13; *see Bailey*, 228 F.3d at 344 (listing purchase records, bank records, records concerning requirements of filing

health care claims, and records of patients whose services were billed to particular insurance companies); *id.* at 351 (noting that patient records involved were subject to agreement to release information to insurance companies); *Doe*, 253 F.3d at 260-61 (listing bank and financial records of Doe and family members, tax records, patient referral records, and records concerning Doe's medical education).

In sum, contrary to the Government's argument, the compelled production of evidence through use of a subpoena is not analytically distinct from a search for evidence. Both approaches require inquiry into a target's reasonable expectation of privacy. To hold otherwise would be to suggest that government agents can evade the warrant requirement of the Fourth Amendment whenever it is convenient for them to do so, by "compelling production" of rather than searching for the evidence they seek.

CONCLUSION

In sum, stored e-mail surveillance by the government on less than probable cause violates the Fourth Amendment. Compelling a service provider to produce a person's e-mail does not entitle government agents to evade constitutional prerequisites. A holding to the contrary would eviscerate the privacy of modern communications.

Respectfully submitted,

_____

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

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

Counsel for Amici Curiae

Dated: November 21, 2006

APPENDIX – LIST OF AMICI[1]

Ann Bartow
Associate Professor of Law
University of South Carolina School of Law

Patricia L. Bellia
Lilly Endowment Associate Professor of Law
Notre Dame Law School

Eric. B. Easton
Professor of Law
University of Baltimore School of Law

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

Jennifer S. Granick
Director and Instructor of the Stanford Cyberlaw Clinic
Stanford Law School

Stephen E. Henderson
Associate Professor
Widener University School of Law

Deirdre Mulligan
Director, Samuelson Law, Technology and Public Policy Clinic
University of California, Berkeley,
Boalt Hall School of Law

Charles B. Meyer
Visiting Professor of Law
University of Houston Law Center

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

[1] Affiliations for identification purposes only.

Michael L. Rustad
Thomas F. Lambert, Jr. Professor of Law
Suffolk University Law School

Pamela Samuelson
Chancellor's Professor of Law and Information Management
University of California, Berkeley

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

Katherine J. Strandburg
Associate Professor of Law
DePaul University College of Law

Peter Swire
C. William O'Neill Professor of Law
Moritz College of Law of the Ohio State University

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

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing brief complies with the type-volume limitation provided in Rule 32(a)(7)(C)(i) of the Federal Rules of Appellate Procedure. This brief contains 6,993 words of Times New Roman (14 point) proportional type and was prepared using Microsoft Word.

_____

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

CERTIFICATE OF SERVICE

I hereby certify that the foregoing brief for *Amici Curiae* Professors of Electronic Privacy Law and Internet Law was served this 21st day of November, 2006, by first-class mail upon counsel for defendant-appellant and counsel for plaintiff-appellee at the addresses below, and that, pursuant to Fed. R. App. P. 25(a)(2)(B)(i), said brief was filed by dispatching an original and six paper copies via express courier to the Clerk of the Court.

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

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

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

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

_____

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