In the

UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

No. 02-1238
Criminal

UNITED STATES,
Appellant

v.

Dale Robert BACH,
Appellee

Appeal from the United States District Court
for the District of Minnesota

AMICUS CURIAE BRIEF OF PROFESSOR ORIN S. KERR IN SUPPORT OF THE APPELLANT

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

TABLE OF CONTENTS

CASES

STATUTES

OTHER AUTHORITIES

RULES

TREATISES

STATEMENT OF INTEREST

Amicus is a law professor who teaches and writes in the area of computer crime law. This appeal raises two critically important questions of first impression concerning how the Fourth Amendment applies to the Internet. Amicus believes that it is important that the Court have a complete understanding of the complex issues raised by this appeal, and of how the outcome of this appeal is likely to influence the development of electronic privacy law. Amicus has no interest in the outcome of this litigation except as it relates to these concerns.

SUMMARY OF ARGUMENT

The Government's brief largely ignores two difficult and very important questions of Fourth Amendment law raised by this appeal: Does an Internet user have a "reasonable expectation of privacy" in remotely stored files held by an Internet service provider? And if the answer to that question is yes, should the Fourth Amendment "reasonableness" analysis of a court order compelling disclosure follow subpoena precedents or warrant precedents? The Government's brief touches on these two issues, but does not develop them. Instead, the Government tries to offer narrower grounds upon

which this Court nonetheless should reverse the District Court.

The Government is correct that the District Court's order should be reversed. Further, reaching such a result on narrow grounds would permit this Court to resolve this appeal without wading into the difficult issues this case otherwise presents. However, if the Court is inclined to affirm the District Court's order, or otherwise finds the government's narrow argument unpersuasive, the Court may have to answer one or both of these questions. This brief attempts to explain both sides of the debate on these two questions to help the Court address them if it feels it must.

ARGUMENT

I. THE FIRST ISSUE RAISED BY THIS APPEAL IS ONE OF THE MOST IMPORTANT QUESTIONS CONCERNING THE FOURTH AMENDMENT AND THE INTERNET: DOES AN INTERNET USER HAVE A "REASONABLE EXPECTATION OF PRIVACY" IN THEIR REMOTELY STORED FILES HELD BY AN INTERNET SERVICE PROVIDER SUCH AS YAHOO?

The Government's brief focuses on whether the Government's conduct was "reasonable." Because the Government's conduct was not "unreasonable," it argues, the Government did not violate the Fourth Amendment. See Appellant's Br. at 13-23. However, the Fourth Amendment does not prohibit acting unreasonably in the abstract; rather, it prohibits "unreasonable searches and seizures." U.S. Const.

Amend. IV. As a result, this Court's first analytical step should be to determine whether the Government's conduct amounted to a Fourth Amendment "search" or "seizure." See Smith v. Maryland, 442 U.S. 735, 739 (1979). This in turn hinges upon whether the government's conduct violated the defendant's "reasonable expectation of privacy." See id. at 740 (citing Katz v. United States, 389 U.S.347, 361 (1967) (Harlan, J., concurring)).[1]

The question is a surprisingly difficult one. It is difficult because the Supreme Court has repeatedly held that the Fourth Amendment does not protect information revealed to third parties. See Smith, 442 U.S. at 743-44; United States v. Miller, 425 U.S. 435, 443 (1976); Couch v. United States, 409 U.S. 322, 335 (1973); Hoffa v. United States, 385 U.S. 293, 302 (1966). As the Court stated in Miller,

> the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Miller, 425 U.S. at 443 (citations omitted).

Several courts have applied this rationale to hold that an Internet user does not retain a reasonable expectation of

[1] The Government's brief hints at this fundamental question in various places, see Appellant's Brief at 16 n.6., 29-30, but does not develop the argument.

privacy in non-content information disclosed to an Internet service provider ("ISP").[2] See Guest v. Leis, 225 F.3d 325, 335-36 (6th Cir. 2001) (finding no expectation of privacy in non-content information disclosed to ISP) ; United States v. Hambrick, 55 F. Supp.2d 504, 508-09 (W.D.Va. 1999), aff'd 225 F.2d 656 (4th Cir. 2000) (unpublished opinion) (same); United States v. Kennedy, 81 F. Supp.2d 1103, 1110 (D.Kan. 2000) (same).

The rationale of these cases is that by communicating with their ISPs, Internet users have revealed information to their ISPs and have relinquished their Fourth Amendment rights in that information. See, e.g., Leis, 225 F.3d at 335-36.

---

[2]In this Brief, "content" will refer to the actual message, whereas "non-content information" refers to mere information about the message. For example, the envelope of a letter contains non-content information such as the "to" and "from" address, and the postmark; in contrast, the "content" is the letter itself, tucked into the sealed envelope. The same content/non-content distinction can be made for telephone communications and e-mails. In the case of e-mails for, example, contents are the actual message, and non-content information would include the "to" and "from" e-mail address and any logs recording when the e-mail was sent and received.

The federal statutory regime that regulates e-mail and telephone privacy follows the same distinction. Compare 18 U.S.C. § 2511 (prohibiting the real-time interception of the contents of e-mails and telephone calls) and 18 U.S.C. § 2703(a),(b) (regulating access to the contents of stored e-mails and voice mails) with 18 U.S.C. § 3121 (prohibiting the real-time acquisition of non-content "dialing, routing, addressing, and signalling information" relating to e-mails and telephone calls) and 18 U.S.C. § 2703(c) (regulating access to stored non-content records of e-mails and telephone calls).

This approach matches the rationale applied by this Court when it held that the Fourth Amendment does not protect account records belonging to customers of the phone company and Western Union. See United States v. Fregoso, 60 F.3d 1314, 1321 (8th Cir. 1995) (holding that telephone company customers do not retain a reasonable expectation of privacy in account information held by the telephone company); In Re Grand Jury Proceedings, 827 F.2d 301, 302-03 (8th Cir. 1987) (holding that Western Union customers have no reasonable expectation of privacy in Western Union records concerning the customers' activities).

The key question is, does this rationale also apply to content information such as e-mails, and if so, when? If the rationale applies, an Internet user will not have a reasonable expectation of privacy in remotely stored files, and the government's conduct in this case was not a "search" or "seizure" and could not have violated the Fourth Amendment. If the rationale does not apply, however, an Internet user may have such an expectation of privacy, a "search" and "seizure" may have occurred, and the government's conduct may have violated the Fourth Amendment.

The Supreme Court has established that the disclosure rationale generally does not apply to contents in the case of postal letters and traditional telephone calls. The Court has

held that a postal mail and telephone user does ordinarily retain Fourth Amendment protection in content information, but not non-content information. Compare Berger v. New York, 388 U.S. 41 (1967) (finding Fourth Amendment protection in the contents of telephone conversations) and Ex Parte Jackson, 96 U.S. (6 Otto) 727, 733 (1877)(concluding that the Fourth Amendment protects sealed postal letters) with Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (finding no Fourth Amendment expectation of privacy in telephone pen register information) and United States v. Huie, 593 F.2d 14, 15 (5th Cir. 1979)(finding no Fourth Amendment protection in the non-content information on the outside of postal letters).

Although the reasons for this distinction have been questioned, the different treatment for content and non-content information typically has been justified on the ground that in the case of the postal system and traditional telephone network, the content information is "sealed," non-visible to the network operators, whereas non-content information is exposed to the network operator in the course of delivery, and thus disclosed to a third-party. See, e.g., Smith, 442 U.S. at 744. In the case of a postal letter, the Postal Service sees the outside of a sealed envelope, but not the contents of the letter inside. See Huie, 593 F.2d at 15. Similarly, in the case of a traditional telephone call, the

phone company sees the number dialed, but once it connects the call it completes a closed circuit between the two callers and no longer sees the call.

Unlike the traditional telephone network and postal mail system, however, the Internet does not treat content and non-content information differently. The content is not sealed; both content and non-content information are disclosed to the ISP in a steady stream of data. See Preston Gralla, How the Internet Works 87 (2001). While a casual user may think of e-mail as the equivalent of sealed postal mail, in fact e-mail works more like a postcard: the content of the message is openly visible to the operators of the network. See Simson Garfinkel, PGP: Pretty Good Privacy 8-9 (1995).

A stored e-mail held by an ISP such as Yahoo is simply a captured stream of computer data that the ISP has seen, saved, and stored as a computer file on its server, awaiting retrieval by an account holder with the right username and password. When the account holder logs on to the ISP and accesses the e-mail, the ISP runs off a copy of the computer file and sends the copy electronically to the account holder. See Gralla, at 78-87.

The question is, do these details about how the Internet actually works make a constitutional difference? If the Court chooses to focus on the specifics of how the Internet works,

remotely stored e-mail files probably should not receive protection because they are disclosed to the ISP. This Court and several other Courts of Appeal have followed such an approach when analyzing whether the Fourth Amendment protects cordless telephone calls. Despite the general rule that telephone calls are protected by the Fourth Amendment, see Berger, calls made either to or from cordless telephones are not protected by the Fourth Amendment because cordless telephones calls are broadcast over radio waves, and therefore are exposed to others in the course of transmission. See, e.g., Tyler v. Berodt, 877 F.2d 705, 707 (8th Cir. 1989) (involving a call from a cordless phone); McKamey v. Roach, 55 F.3d 1236, 1239-40 (6th Cir. 1995); United States v. McNulty, 47 F.3d 100, 104-106 (4th Cir. 1995) (involving a call made to a cordless telephone user); United States v. Smith, 978 F.2d 171, 177-81 (5th Cir. 1992).[3]

Alternatively, this Court could focus less on the details of how the technology works, and instead try to match the constitutional rules of the Internet to the older rules for the postal network and the telephone. In this case, remotely stored e-mail files should receive Fourth Amendment

[3] Of course, Congress can protect such calls when the Fourth Amendment does not. In the case of cordless telephone calls, Congress added statutory protection against their interception in 1994. See McKamey, 55 F.3d at 1238 n.1.

protection. See, e.g., Kyllo v. United States, 533 U.S. 27, 34 (2001)(suggesting that as technology advances, the courts should interpret the Fourth Amendment to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."). Whether or not e-mail is technically "sealed," the truth remains that Americans use e-mail just like they use the postal mail. Accordingly, the recognized expectation of privacy in the latter should apply to the former as well. See Katz, 389 U.S. at 352 ("To read the Constitution more narrowly is to ignore the vital role that the [technology in question] has come to play in private communication."); Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) ("Can it be that the Constitution affords no protection against such invasions of individual security?").[4]

If the court is looking for a more doctrinal and less theoretical focus, it might ask whether e-mail sent to an ISP

[4] In a forthcoming law review article, I argue that the question of whether remotely stored files should receive Fourth Amendment protection boils down to whether the Court wishes to follow reality or virtual reality. See Orin S. Kerr, The Problem of Perspective In Internet Law, 91 Geo. L. J. (forthcoming Feb. 2003). If a Court follows physical-world reality, it will conclude that e-mails are disclosed to the ISP, and thus do not retain Fourth Amendment protection. However, if the Court follows virtual reality, it will conclude that e-mails are the equivalent of postal mail and therefore do retain Fourth Amendment protection. A current draft of this paper can be viewed and downloaded from the Internet at http://papers.ssrn.com/abstract=310020.

is better analogized to sealed postal mail or a postcard. Should the Court analogize e-mails to sealed letters and packages, in which case the Fourth Amendment protects them, or unsealed postcards, in which it doesn't?

Of course, even this simple question raises more subtle ones. For example, if the Fourth Amendment can protect remotely stored files, does the protection depend on what kind of remotely stored file is at issue? On whether the user is a paying customer, or the ISP offers the service for free? On whether the file is in a user's inbox, or whether it has been read and placed in the "trash" box? On whether the files are encrypted, arguably "sealing" the letters? On whether the user has complied with the ISP's Terms of Service? See Note, C. Ryan Reetz, Warrant Requirement For Searches Of Computerized Information, 67 B.U. L. Rev. 179 (1987). See also James X. Dempsey, The Fourth Amendment and the Internet, 632A PLI/Pat 735, 741-42, 754 (2001); Orin S. Kerr, The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?", 33 Conn. L. Rev. 503 (2001).

Surprisingly, no Article III court has answered whether and when an Internet user has a reasonable expectation of privacy in remotely-stored files.[5] The only court that has

[5] In the last few years, Courts have decided many cases considering Fourth Amendment protection in computers. For

ruled on this question directly is an Article I court, the U.S. Court of Appeals for the Armed Forces. In United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996), the Court ruled that an America Online (AOL) user does retain a reasonable expectation of privacy in e-mails stored with AOL. The Court reasoned that "e-mail is like a letter. It is sent and lies sealed in the computer until the recipient opens his or her computer and retrieves the transmission." See id. at 418. Accordingly, unopened e-mail received the same Fourth Amendment protection as unopened postal mail. See id.

The result in Maxwell is certainly plausible, but the analysis seems to beg the question: *does* e-mail lie sealed in the computer? Hasn't the content of the e-mail actually been

---

example, Courts have analyzed the Fourth Amendment rights of employees in their workplace computers (both government employees, see United States v. Simons, 206 F.3d 392 (4th Cir. 2000), and private sector employees, see Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002)). Courts have also ventured (albeit unconvincingly) into whether computer bulletin board users have privacy rights in their user of a "bannered" remote computer bulletin board, see Leis, 225 F.3d at 333 (answering "no"), and whether students generally have privacy rights in their use of university computers, see United States v. Butler, 151 F. Supp.2d 82 (D. Me. 2001) (answering "no").

But unless we construe the District Court's order as an implicit ruling in the affirmative, no Article III court has ruled on whether an Internet user has a reasonable expectation of privacy in files held remotely by an ISP. But see United States v. Hambrick, 2000 WL 1062039 at *4 (suggesting in dicta that there may be a distinction between content and non-content information in the context of e-mail). Cf. United States v. Lamb, 945 F. Supp. 441, 455 n.9 (N.D.N.Y. 1996) (assuming but not deciding that an AOL user has a reasonable

seen by lots of computers before it reaches the ISP? See Smith, 442 U.S. at 744-45 (concluding that conveying information to the phone company's electronic machinery relinquishes Fourth Amendment protection in the information just as it would if the disclosure were to a phone company employee); McNulty, 47 F.3d at 104-106.

Nor are these merely academic questions. The answers will have a direct impact on the constitutionality of existing federal legislation on e-mail privacy. Following Miller and Smith v. Maryland, Congress generally has assumed that privacy protections for Internet communications are primarily statutory questions for Congress, not constitutional questions for the courts. See S.Rep. 99-541, reprinted at 1986 U.S.C.C.A.N. 3555, 3557 (citing Miller). In 1986, Congress enacted a complex statutory framework that protects electronic communications and stored e-mails. See 18 U.S.C. § 2701-11 (The Electronic Communications Privacy Act, which protects stored e-mails, voicemails, and non-content records); 18 U.S.C. § 2510-22 (The Wiretap Act, also known as "Title III," which protects the contents of e-mails and telephone calls in transit); 18 U.S.C. § 3121-27 (The Pen Register and Trap and Trace Devices Statute, which protects non-content information about Internet and telephone communications in transit).

---

expectation of privacy in remotely stored files).

On the whole, these three statutes erect a Fourth-Amendment-like set of privacy protections. Although the laws have been tinkered with many times to make them stronger or weaker in various ways -- most recently in October 2001, when Congress passed the USA PATRIOT anti-terrorism act, Pub. L. 107-56 -- the laws protect by statute something akin to what the Fourth Amendment would protect if it did (or perhaps does protect because it does) apply to remotely-stored files.

Despite this, a broad holding by this Court that the Fourth Amendment protects remotely stored files could undercut the constitutionality of several provisions of this legislative scheme. The reason is that Congress chose not to protect all stored e-mails with a full warrant requirement. Instead, Congress opted to require law enforcement to obtain a search warrant to obtain some e-mails, but permitted lesser process such as an "articulable facts" court order or even a subpoena to obtain other stored e-mails. See 18 U.S.C. § 2703. In particular, 18 U.S.C. § 2703(a) requires the government to obtain a search warrant to compel an ISP to divulge unopened e-mails held in storage for less than 180 days. See 18 U.S.C. § 2703(a). Once an e-mail has been stored unopened for 180 days, however, the government can compel the ISP to divulge the e-mail with either a subpoena or an "articulable facts" court order pursuant to § 2703(d) combined with prior notice

to the subscriber. No warrant is required. See id. Further, once the e-mail has been opened, and is no longer held "incident to transmission" by the ISP but rather is simply a remotely stored file, the statutory protection changes. At that point, the government can compel opened e-mail from a provider "to the public" with a subpoena or articulable facts court order plus notice, see § 2703(b).[6]

This statutory scheme appears to reflect Congress's judgment that not all remotely stored files receive Fourth Amendment protection. See Clifford S. Fishman & Anne T. McKenna, Wiretapping and Eavesdropping § 26:9, at 26-12 (2d ed. 1995). Of course, that is ultimately a question for the Courts, not Congress. See Marbury v. Madison, 5 U.S. (1 Cranch) 137 (1803). Perhaps the Constitution requires a warrant in all cases, not just some, and parts of 18 U.S.C. § 2703 are in fact unconstitutional. If so, this Court should not hesitate to reach such a result; such a decision could lay the foundation for a strong Fourth Amendment in cyberspace.

On the other hand, in light of the complex legislative framework Congress has enacted, judicial caution may be warranted. Cf. McNulty, 47 F.3d at 104 (rejecting a claim of

[6] A comprehensive explanation of this statutory scheme appears in Chapter 3 of United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2001) (available at www.cybercrime.gov/searchmanual.htm).

constitutional protection in calls to a cordless phone user, in part on the ground that holding to the contrary would force the court "to rule the statutory exceptions of Title III unconstitutional," an "untoward result" given the "heavy presumption of constitutionality that attaches to the carefully considered decisions of a coequal and representative branch of our Government.") (internal quotations and brackets omitted).

II. BEFORE DETERMINING WHETHER THE GOVERNMENT'S CONDUCT WAS "REASONABLE," THIS COURT SHOULD FIRST DECIDE WHETHER THE FOURTH AMENDMENT "REASONABLENESS" ANALYSIS SHOULD FOLLOW SEARCH WARRANT PRECEDENTS OR SUBPOENA PRECEDENTS.

Assuming Fourth Amendment protection in remotely stored files, the second difficult question underlying this appeal considers whether the statutory court order process found in 18 U.S.C. § 2703 is governed by the Fourth Amendment precedents for search warrants or subpoenas. The answer to this question will determine whether the court should apply the forgiving reasonableness standards that the Supreme Court has established for subpoenas, or the more strict reasonableness standards that the Court has established for warrants.[7]

[7] The Government touches on this argument in its brief, but again does not develop it. See Appellant's Brief at 26-27

The question is important because the Supreme Court has created two distinct lines of Fourth Amendment precedents that govern the acquisition of evidence in criminal cases. See In re Subpoena Duces Tecum, 228 F.3d 341, 346-49 (4th Cir. 2000) (summarizing cases); In re Horowitz, 482 F.2d 72, 75-80 (2d Cir. 1973) (Friendly, J.) (summarizing cases). The first line of cases involves search warrants, which authorize the government to enter private property and search the property for evidence described in the warrant. See, e.g., Andresen v. Maryland, 427 U.S. 463 (1976). See also Fed. R. Crim. P. 41. The second line of precedents involves subpoenas, court orders that compel the recipient to locate and divulge information to the government with a period of time. See e.g., United States v. Dionisio, 410 U.S. 1, 7-12 (1973); Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186, 209 (1946); Hale v. Henkel, 201 U.S. 43, 76 (1906).

The Fourth Amendment's "reasonableness" requirement assumes a very different form for compelled disclosures pursuant to subpoenas than it does for direct searches pursuant to traditional search warrants. See Dionisio, 410 U.S. at 10. In the context of subpoenas, "reasonableness" generally requires only that the subpoena be reasonably

---

("[T]he ECPA treats a search warrant for email records more like a subpoena . . . ").

related to a legitimate government purpose, not violate a legally recognized privilege, and not be so broad that it would be overly burdensome for the recipient of the subpoena to comply with it. See, e.g., Donovan v. Lone Steer, Inc., 464 U.S. 408, 412-16 (1984); In re Subpoena Duces Tecum, 228 F.3d at 349 (noting the standard, as well as the slight variations that courts apply depending on the circumstances).[8]

According to the Supreme Court, the reason that the Fourth Amendment reasonableness standards are much less strict in the case of compelling information or appearance pursuant to a subpoena than in the case of a direct search or arrest pursuant to a warrant is that

> [t]he latter is abrupt, is effected with force or the threat of it and often in demeaning circumstances, and, in the case of arrest, results in a record involving social stigma. A subpoena is served in the same manner as other legal process; it involves no stigma whatever; if the time for appearance is inconvenient, this can generally be altered; and it remains at all times under the control and supervision of a court.

Dionisio, 410 U.S. at 10 (quoting United States v. Doe, 457 F.2d 895, 898 (2d Cir. 1972) (Friendly, J.)).

[8] Whether the item identified in the subpoena is protected by a "reasonable expectation of privacy" becomes only a threshold question; if a person has a reasonable expectation of privacy in the item subpoenaed, the person has standing to challenge the subpoena under the subpoena standard. Otherwise, the person has no Fourth Amendment standing to challenge the subpoena. See United States v. Plunk, 153 F.3d 1011, 1020 (9th Cir. 1998); United States v. Phibbs, 999 F.2d 1053, 1077 (6th Cir. 1993).

This appeal raises difficult questions of which set of precedents to follow because although the court order obtained in this case is called a "warrant," it is actually a hybrid between a search warrant and a subpoena. Section 2703(a) creates this unique hybrid: court orders that are obtained like search warrants but executed like subpoenas. When it enacted § 2703(a), Congress attempted to regulate law enforcement by requiring it to have probable cause before obtaining a court order to compel certain types of contents from ISPs. See 18 U.S.C. § 2703(a). Congress created by statute what is in effect a glorified subpoena -- a subpoena issued only when a neutral magistrate finds probable cause.

The resulting order is part subpoena, part search warrant. The order is obtained like a search warrant: an affiant appears before a neutral magistrate, who reviews the application like any other search warrant application. On the other hand, the order is executed like a subpoena: agents do not knock down the door of the ISP and look for the evidence themselves in an "abrupt" or "forceful" way, but rather fax or mail the signed order to the ISP just as they would serve a subpoena. See United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations n.8 (2001) (available at www.cybercrime.gov/searchmanual.htm) ("Although both are

called ‘search warrants,’ they are very different in practice. ECPA search warrants required by 18 U.S.C. § 2703(a) are court orders that are served much like subpoenas: ordinarily, the investigators bring the warrant to the provider, and the provider then divulges the information described in the warrant to the investigators within a certain period of time.”)

Which standards of reasonableness apply to this hybrid order? For Fourth Amendment purposes, should this Court focus on the way in which the order was obtained, and the label Congress assigned (a “warrant”), or should it focus on the way the order was actually executed? Is the court order served on Yahoo really a search warrant, or is it more of a subpoena because it was served like a subpoena? Or does this hybrid order call for a hybrid standard of reasonableness, something less strict than that applied to common search warrants but more strict than that applied to subpoenas? Cf. United States v. Lartey, 716 F.2d 955, 960-63 (2d Cir. 1983)(considering the Fourth Amendment reasonableness standards that apply to the execution of “forthwith” subpoenas).

The questions are further complicated by the fact that the court order to compel evidence is served on a third party. The ISP receives the court order, not the Internet user whose privacy interests are at stake. The courts have had only a

handful of opportunities to consider the Fourth Amendment standards for orders to compel evidence served on third parties.[9] These cases involved subpoenas served on third parties for the defendant's papers, letters, and telegraph messages in the third party's possession.

The results have been mixed. In United States v. Schwimmer, 232 F.2d 855 (8th Cir. 1956), the government served a subpoena on a third-party storage facility that had the defendant's papers in its possession. Henry Schwimmer was a Kansas City lawyer who was suspected of involvement in a tax evasion and public corruption scheme in his role as an attorney. By the time the grand jury investigating the case focused on Schwimmer, Schwimmer had closed his office, boxed up his files, and placed them in storage before going to Puerto Rico. See id. at 858-59. The grand jury served two subpoenas on the storage company, ordering it to disclose books, records and files of Harry Schwimmer either on its premises or under its control. See id. at 859. Schwimmer

[9] It may be helpful to understand why such cases are rare. In the majority of cases in which defendants hand over documents and other information to third parties, the handing over constitutes a Fourth Amendment "disclosure" and the defendant loses his reasonable expectation of privacy in the documents or information. See, e.g., Miller and Couch. If no Fourth Amendment protection exists, courts need not evaluate how the reasonableness standard applies when the third party is served with an order to disclose the documents or information to the government.

learned of the subpoenas, and returned to Missouri to challenge the subpoenas on the ground that they violated his Fourth Amendment rights. See id.

This Court held that Schwimmer had standing to challenge the subpoenas, see id. at 862;[10] that the first subpoena was constitutionally unreasonable because it was merely part of "an abstract hunt for possible crime in Schwimmer's legal practice," id.; and that the second more narrow subpoena complied with the Fourth Amendment, see id. at 863-63. Although the Court formally expressed the reasonableness inquiry in remarkably cryptic language, see id. at 861, in practice it seems to have applied the usual subpoena reasonableness standard, rather than a search warrant standard. See also United States v. Allison, 619 F.2d 1254 (8th Cir. 1980) (evaluating service of subpoena served on custodian of union records under subpoena standard); United States v. Barr, 605 F. Supp. 114, 119 (S.D.N.Y. 1985) (applying subpoena reasonableness standard to subpoena served on private third-party mail service for the defendant's undelivered mail in the third party's possession); Newfield v. Ryan, 91 F.2d 700, 702-05 (5th Cir. 1937) (permitting subpoena served on telegraph company for copies of defendants'

[10] In modern parlance, this would mean that he had a reasonable expectation of privacy in the papers, and thus had standing to challenge the subpoena. See Phibbs, 999 F.2d at

telegrams in the telegraph company's possession).

These cases suggest that at least in the subpoena context, the basic reasonableness analysis probably does not change when the subpoena is served on a third party. However, at least one court has held that in the context of an administrative subpoena, the presence of a third party with no incentive to challenge the subpoena does change the reasonabless standard. In Hell's Angels Motorcycle Corp. v. County of Monterey, 89 F. Supp.2d 1144 (N.D. Cal. 2000), Judge Walker held that the target of the investigation must receive prior notice of the subpoena served on the third-party so that the target may properly challenge the subpoena. See id. at 1151-53 (concluding that "notice and a right to intervene are mandated by the Fourth Amendment whenever a subpoena seeks records in which an individual holds a proprietary or privilege interest"). And of course, these cases all involve subpoenas: no Court has considered how the reasonableness requirement applies to hybrid warrants served like subpoenas on third parties.

Whatever solutions to these complex problems may exist, the District Court's order clearly is not one of them. The District Court's order effectively ruled that the Fourth Amendment forbids Congress from enacting such a hybrid

---

1077.

warrant/subpoena scheme. If Congress wishes to require the police to satisfy a search warrant threshold to obtain a de facto subpoena, the District Court's order indicates, the Fourth Amendment is satisfied only if the police execute the subpoena like a warrant, with an officer present in compliance with 18 U.S.C. § 3105.

This is a strange conclusion. Congress was trying to protect privacy when it enacted § 2703(a); it added a statutory requirement of a hybrid warrant where, precedents indicated, a mere subpoena would probably suffice under the Fourth Amendment. It's hard to see why the Fourth Amendment would prohibit Congress from protecting privacy in this way. Surely the label that Congress chose cannot be dispositive – whether Congress calls the hybrid order a "search warrant" or a "probable cause subpoena" (something that Congress can and has changed over time[11]) cannot be critical to the Fourth Amendment inquiry. See Sibron v. New York, 392 U.S. 40, 59

[11] In fact, Congress recently amended the language used to describe this order. From 1986 until 2001, the required order was called "a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant." 18 U.S.C. 2703(a) (1994). In October of 2001, as part of the USA Patriot Act, Congress amended the language so that now it requires "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant." 18 U.S.C. § 2703(a) (2002). The change apparently reflects an attempt to clarify that the order is not a traditional Rule 41 search warrant, but rather merely a hybrid order issued using the procedures of Rule 41.

(1968) (noting that while the legislature is "free to develop its own law of search and seizure . . . , and in the process it may call the standards it employs by any names it may choose," what matters under the Fourth Amendment is not "the labels which [the legislature] attaches to such conduct," but rather "whether the search was reasonable under the Fourth Amendment").

CONCLUSION

There are many ways in which this Court can resolve this appeal. Some are broad, others are narrow. Whatever approach the Court prefers, the undersigned Amicus respectfully submits that two principles should guide this Court.

First, clarity is important. This Court should carefully explain which of the issues raised by the appeal it feels must be resolved, and which issues it will leave for another day. Given the complex and interconnected issues raised by this appeal, analytic clarity will help other courts, Congress, and scholars alike understand the scope and consequences of the Court's decision.

Second, undersigned Amicus respectfully submits that judicial caution will likely serve this area of law more effectively than judicial boldness. As the Second Circuit has noted recently in the First Amendment context, the application

of constitutional protections to the Internet best calls for narrow holdings, reflecting our limited knowledge of potentially far-reaching consequences:

> A more evolutionary approach, involving the accretion of case-by-case judgments, could produce fewer mistakes on balance, because each decision would be appropriately informed by an understanding of particular facts.

Name.Space, Inc. v. Network Solutions, Inc., 202 F.3d 573, 584 n. 11 (2d Cir.2000) (quoting Cass R. Sunstein, The Supreme Court, 1995 Term-Foreword: Leaving Things Undecided, 110 Harv. L. Rev. 4, 18 (1996)). This is all the more true given the complex statutory scheme Congress has created to protect e-mails. See McNulty, 47 F.3d at 104. See also Adams v. City of Battle Creek, 250 F.3d 980, 986 (6th Cir. 2001) ("The Electronic Communications Privacy Act is part of detailed legislative scheme under Title III of the Omnibus Crime and Control Act of 1986. The legislation seeks to balance privacy rights and law enforcement needs, keeping in mind the protections of the Fourth Amendment against unreasonable search and seizure. Congress made the Act the primary vehicle by which to address violations of privacy interests in the communication field.").

STATEMENT CONCERNING ORAL ARGUMENT

The undersigned Amicus assumes that counsel for the

United States will be prepared to discuss the issues raised in this brief at oral argument, and therefore that participation by the undersigned in oral argument is unnecessary. If the Court wishes Amicus to participate, however, the undersigned Amicus would be available to do so pursuant to Fed. R. App. P. 28(g).

CERTIFICATE OF COMPLIANCE

The undersigned Amicus hereby certifies that this brief contains approximately 5,000 words, and therefore complies with the 7,000 word maximum imposed on amicus curiae briefs by Fed. R. App. 29(d) and Fed. R. App. P. 32(a)(7)(i). The brief was prepared using Microsoft Word 97.

Dated: June 4, 2002.

Respectfully submitted,

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