

No. 02-1238, Criminal

In the United States Court of Appeals for the Eighth Circuit

UNITED STATES OF AMERICA,

Appellant,

v.

DALE ROBERT BACH,

Appellee.

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

Brief of *Amicus Curiae* Electronic Privacy Information Center
in Support of Appellee, Dale Robert Bach, Urging Affirmance

MARC ROTENBERG
MIKAL CONDON
ELECTRONIC PRIVACY INFORMATION
CENTER
1718 Connecticut Ave., NW, Suite 200
Washington, D.C. 20009
(202) 483-1140

Counsel for *Amicus Curiae*

**IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT**

UNITED STATES OF AMERICA,)	
)	No. 02-1238, Criminal
Appellant,)	
)	
)	
v.)	
)	
)	
DALE ROBERT BACH,)	
)	
Appellee.)	
)	

**MOTION OF *AMICUS CURIAE* ELECTRONIC PRIVACY
INFORMATION CENTER FOR LEAVE TO FILE ACCOMPANYING
*AMICUS BRIEF***

Pursuant to Federal Rule of Appellate Procedure Rule 29(b), *amicus curiae* Electronic Privacy Information Center (“EPIC”) requests leave to file the accompanying *amicus curiae* brief in support of Appellee. This brief urges affirmance of the District Court’s decision. Appellee Dale Robert Bach has consented to the filing of this brief; appellant United States has declined to give its consent.

The Electronic Privacy Information Center is a public interest research center in Washington, D.C. that was established to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and

other constitutional values. EPIC has participated as amicus curiae in numerous privacy cases, including most recently *Watchtower Bible and Tract Soc’y of N.Y., Inc. v. Vill. of Stratton*, 122 S. Ct. 2080 (2002). In this case, a law enforcement officer failed to comply with a well-established statutory requirement when he faxed a warrant to an e-mail service provider. This failure to observe statutorily mandated procedures violated appellee's Fourth Amendment privacy rights, and the court's resolution of this case could potentially affect the privacy interests of millions of citizens.

As there are today more than 140 million internet users in the United States who could become subject to such warrants issued from a fax machine, EPIC believes it is vital to understand the history of the requirement that a police officer be physically present when a search warrant is served and therefore respectfully requests that this Court grant it leave to file the accompanying *amicus curiae* brief.

Dated: July 26, 2002

Respectfully submitted,

MARC ROTENBERG
MIKAL CONDON
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Ave., NW, Suite 200
Washington, D.C. 20009
(202) 483-1140

Counsel for *Amicus Curiae*

TABLE OF CONTENTS

TABLE OF CONTENTS.....	iii
TABLE OF AUTHORITIES.....	iv
STATEMENT OF THE AMICUS CURIAE.....	1
SUMMARY OF THE ARGUMENT.....	1
QUESTION PRESENTED.....	3
ARGUMENT.....	4
I. The Fourth Amendment has Always Required the Presence of a Police Officer for the Service of a Search Warrant	4
II. Section 3105 Requires the Presence of a Police Officer During the Service of a Warrant and This Circuit has Made Clear that State Officers Must Comply With the Statutory Obligation.....	9
III. The Fourth Amendment Requires That A Law Enforcement Officer Personally Serve A Warrant For A Search Of An E-Mail Service Provider’s Remotely Stored Files.....	11
A. Law Enforcement Officers Must Observe Fourth Amendment Procedures to Secure the Privacy Interests of Internet Users.....	11
B. Because An E-Mail Provider Is Immune From Liability Stemming From Its Cooperation With A Warranted Search, It Is Imperative To Foster Accountability By Preserving The Formalities Associated With Service Of A Search Warrant.....	14
CONCLUSION.....	17

TABLE OF AUTHORITIES

CASES

<i>Boyd v. United States</i> , 116 U.S. 616 (1886).....	4, 6
<i>Byars v. United States</i> , 273 U.S. 28 (1927).....	7
<i>Elkins v. United States</i> , 364 U.S. 206 (1960).....	9, 10
<i>Gouled v. United States</i> , 255 U.S. 298 (1921).....	5
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	11, 13
<i>Keehn v. United States</i> , 300 F. 493 (1st Cir. 1924).....	8
<i>Kyllo v. United States</i> , 533 U.S. 27, 33 (2001).....	12
<i>Massachusetts v. Sbordone</i> , 424 Mass. 802 (Mass. 1997).....	15
<i>McVeigh v. Cohen</i> , 983 F. Supp. 215 (D.D.C. 1998).....	8
<i>Morris v. Florida</i> , 622 So.2d 67 (Fla. App. 1993).....	15
<i>Ohio v. Rubinette</i> , 519 U.S. 33 (1996).....	14
<i>Smith v. Maryland</i> , 442 U.S. 735, 743-744 (1979).....	12
<i>Steele v. United States</i> , 267 U.S. 505 (1925).....	7
<i>United States v. Appelquist</i> , 145 F.3d 976 (8th Cir. 1998).....	10
<i>United States v. Bieri</i> , 21 F.3d 811 (8th Cir. 1994).....	10
<i>United States v. Knights</i> , 122 S. Ct. 587 (2001).....	14
<i>United States v. Lefkowitz</i> , 285 U.S. 452 (1932).....	14
<i>United States v. Maxwell</i> , 45 M.J. 406 (C.A.A.F. 1996).....	12

<i>United States v. Moore</i> , 956 F.2d 843 (8th Cir. 1992).....	10
<i>United States v. Murphy</i> , 69 F.3d 237 (8th Cir. 1995).....	10, 11
<i>United States v. Ramirez</i> , 523 U.S. 65 (1998).....	10
<i>United States v. Schwimmer</i> , F. Supp. 119 (E.D.N.Y. 1988).....	15
<i>Washington v. Kern</i> , 81 Wash. App. 308, 914 P.2d 114 (Wash. App. 1996).....	15
<i>Watchtower Bible and Tract Soc’y of N.Y., Inc. v. Vill. of Stratton</i> , 122 S. Ct. 2080 (2002).....	8
<i>Weeks v. United States</i> , 232 U.S. 383 (1914).....	4, 5, 8, 9
<i>Wyoming v. Houghton</i> , 526 U.S. 295 (1999).....	14

LEGISLATIVE HISTORY AND STATUTES

Regulation of the Collection of Duties on Tonnage and on Merchandise, 1 Cong. Ch. 5; 1 Stat. 29 (1789).....	5, 6
Revenue Act of 1863. 12 Stat. 737 (1863).....	6
Espionage Act of 1917, Title XI, Pub. L. No. 65-24, 40 Stat. 229.....	7
National Prohibition Act of 1923 (Volstead Act), 41 Stat. 305.....	6
National Prohibition Act, 42 Stat. 222 (1924).....	8
18 U.S.C. § 617.....	7
18 U.S.C. § 2703(e)	16
18 U.S.C. § 3105	7, 9
18 U.S.C. § 3109	10

BOOKS AND ARTICLES

2 Wayne R. LaFave, *Search & Seizure* § 4.8(a), 599-600 (3d ed. 1996)10

James X. Dempsey, *The Fourth Amendment and the Internet, in First Annual Institute on Privacy Law Strategies for Legal Compliance in a High Tech and Changing Regulatory Environment* 1017 (John B. Kennedy & Paul M. Schwartz ed., Practising Law Institute 2000).....2

Patricia Fusco, *Top U.S. ISPs By Subscriber* (May 29, 2002) at <http://www.isp-planet.com/research/rankings/usa.html> (last accessed June 13, 2002).....2

Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication, 110 Harv. L. Rev. 1591 (1997).....13

Nua.com, *AOL Dominates U.S. ISP Market* (Feb. 11, 2002) at http://nue.ie/surveys/index.cgi?f=VS&art_id=905357646&reltrue (last accessed June 13, 2002).....2

Nua.com, *How Many Online?* (Feb. 2002) at http://www.nua.ie/surveys/how_many_online/index.html (last accessed July 26, 2002)2

Michael Pastore, *Global Census of Online Populations* (March 25, 2002) at <http://www.isp-planet.com/reaserch/2002/census.html> (last accessed June 13, 2002).....2

U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 51-52 (March 2001).....15

Elizabeth Weise, *Electronic Evidence Hot New Topic*, USA Today, May 10, 1999, at 1A.....2

OTHER

Yahoo! Terms of Service at <http://docs.yahoo.com/info/terms> (last accessed July 16, 2002).....12

Yahoo! Privacy Policy at <http://privacy.yahoo.com> (last accessed July 16, 2002).....12

Yahoo! Online Support *at* <http://help.yahoo.com/help/us/mail/access/access-09.html> (last accessed July 16, 2002).....12

STATEMENT OF *AMICUS CURIAE*

Amicus Electronic Privacy Information Center (“EPIC”) is a public interest research center in Washington, D.C. that focuses public attention on emerging civil liberties issues and advocates to protect privacy and constitutional values. EPIC believes that both 18 U.S.C. § 3105 and the Fourth Amendment mandate official presence during the service of a search warrant, a procedural safeguard that is particularly important as emerging technological innovations pose new challenges to personal privacy.

SUMMARY OF ARGUMENT

The search warrant at issue in this case was served without a police officer being present, in direct violation of 18 U.S.C. § 3105, which mandates officer presence at the service of a warrant. Formal procedures—including the requirement of an officer's presence at the service of a search warrant—have been in place since the 1700s to safeguard individuals from unwarranted intrusion upon their privacy by government officials, and to discourage governmental abuse of power by ensuring guarantees of trustworthiness and accountability.

Because a subscriber has an expectation of privacy in e-mail transmitted by an Internet Service Provider (“ISP”), the characteristics of the Internet do not negate the requirement of an officer’s presence for the service of a warrant. It is thus critical that law enforcement officers observe the formalities associated with

service of a search warrant in digital environments. Furthermore, the procedures by which warrants are served for electronic information impact millions of people: more than 540 million people throughout the world were online in 2002, with over 180 million in the United States and Canada alone.¹ The world's largest ISP, America Online, received approximately 20 warrants per month in 1999, a figure that has risen steadily over the course of several years.² Thus, the procedures permitted for the execution of a search warrant on an ISP implicate the Fourth Amendment rights of millions of Internet users.

The application of Fourth Amendment protections to privacy interests in digital environments raises important questions concerning the technical service of

¹ Nua.com, *How Many Online?* at http://www.nua.ie/surveys/how_many_online/index.html (Feb. 2002). There are more than 140 million Internet Service Providers (ISPs) subscribers in the United States alone. *AOL Dominates US ISP Market* at www.nua.ie/surveys/index.cgi?f=VS&art_id=905357646&reltrue (Feb. 11, 2002). The Telecommunications and Information Administration estimates that two million people become new Internet users each month. Patricia Fusco, *Top U.S. ISPs By Subscriber* at www.isp-planet.com/research/rankings.usa.html (May 29, 2002). The Computer Industry Almanac estimates that 945 million people globally will be Internet users by 2004. See Michael Pastore, *Global Census of Online Populations* at <http://www.isp-planet.com/research/2002/census.html> (March 25, 2002).

² Elizabeth Weise, *Electronic Evidence Hot New Topic*, USA Today, May 10, 1999, at 1A. Electronic evidence may comprise as much as thirty percent of all evidence admitted in court. *Id.* During the course of a single 1999 investigation, the FBI seized enough electronic evidence to almost fill the Library of Congress twice. James X. Dempsey, *The Fourth Amendment and the Internet*, in *First Annual Institute on Privacy Law Strategies for Legal Compliance in a High Tech*

a valid search warrant. Law enforcement officers are legally obligated to ensure the privacy rights of individuals. ISPs, on the other hand, are bound by no such obligation and are in fact exempt under 18 U.S.C. § 2703(e) from any liability arising from their participation in a search. Therefore, an officer's presence for the service of a warrant is a crucial procedural safeguard of an individual's Fourth Amendment rights.

QUESTION PRESENTED

When a state officer serves a state warrant upon a third party in violation of a state law mandating official presence at the warrant's service, is the use of the resulting evidence in a federal prosecution prohibited by the United States Constitution and a federal statute similarly requiring official presence during warrant service?

and Changing Regulatory Environment 1017 (John B. Kennedy & Paul M. Schwartz ed., Practising Law Institute 2000).

ARGUMENT

I. The Fourth Amendment has Always Required the Presence of a Police Officer for the Service of a Search Warrant

Since the 1700s, United States law has required an officer's presence during the service of a search warrant. *See Boyd v. United States*, 116 U.S. 616, 624 (1886) (detailing the history of search and seizure law and procedure). An officer's presence discourages government abuse of power and unwarranted intrusion upon privacy by ensuring guarantees of trustworthiness and accountability. The Supreme Court has long recognized the importance of strict adherence to procedural safeguards in the execution of search warrants, because "[i]t may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing ... by silent approaches and slight deviations from legal modes of procedure." *Boyd*, 116 U.S. at 633. (emphasis added). Therefore, "[i]t is the duty of the courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachment thereon." *Id.*

Indeed, as the Supreme Court has long recognized, the Fourth Amendment was adopted as a procedural safeguard against the arbitrary exercise of governmental authority, "securing to the American people, among other things, those safeguards which had grown up in England to protect the people from unreasonable searches and seizures" *Weeks v. United States*, 232 U.S. 383, 391

(1914). *Weeks* heralded the dawning of the constitutional age of criminal procedure, in which the Supreme Court established the exclusionary rule prohibiting introduction of evidence if obtained by federal officers through a procedural violation of Fourth Amendment requirements governing search and seizure. To permit introduction of unlawfully obtained evidence at trial would "affirm by judicial decision a manifest neglect if not an open defiance of the prohibitions of the Constitution, intended for the protection of the people against such unauthorized action." *Id.* at 394. The Court in *Weeks* recognized that prohibiting use by the government of improperly obtained evidence was necessary to ensure that the formalities and procedural safeguards underlying the Fourth Amendment were followed, because "[t]he affect of the Fourth Amendment is to put the courts of the United States and Federal officials in the exercise of their power and authority, under limitations and restraints as to the exercise of such power and authority." *Id.* at 393. Relaxing well-established procedures would lead to "gradual depreciation of the rights secured by [the Fourth Amendment] by imperceptible practice of courts or by well-intentioned but mistakenly over-zealous executive officers." *Gouled v. United States*, 255 U.S. 298, 304 (1921).

In 1789 Congress passed the first statute regulating the collection of import and export duties, thus regulating searches and seizures performed by Federal officers. Regulation of the Collection of Duties on Tonnage and on Merchandise, 1

Cong. Ch. 5; 1 Stat. 29, 43 (July 31, 1789). Under this law, the presence of a collections officer was required at each port. 1 Stat. at 38. The seizure of goods stolen or liable to import duties by an officer of the law “by virtue of a judicial writ” was considered to be within the Fourth Amendment because the individual in possession of such goods had no property right in the items. *See Boyd*, 116 U.S. at 623. The purpose of having an officer present at a search was to ensure that the goods, identified as having been stolen, conformed to the description provided by the rightful owner before they could be seized. *See id.* at 628. Similarly, it was the duty of the customs collector or revenue officer to verify that shipped goods conformed to an invoice or the ship’s manifest. 1 Stat. at 39-43. A search for concealed goods could be performed by an officer, his deputy, or someone else authorized by the officer, but the officer was ultimately responsible for ensuring the legality of the search. 1 Stat. at 44.

Similarly, Congress recognized the necessity of official presence at the service of a warrant when it enacted the Revenue Act of 1863. Although Congress adopted the Act during “a period of great national excitement, when the powers of the government were subjected to a severe strain to protect the national existence,” searches and seizures were governed by the same strict guidelines as before. *Boyd*, 116 U.S. at 621; 12 Stat. 737 (March 3, 1863). Among other safeguards, provisions of the Revenue Act guarded against unreasonable searches and seizures

by mandating that a warrant be served only by a United States marshal or customs official.

The requirements of 18 U.S.C § 3105, the statute at issue here, were adopted almost verbatim from 18 U.S.C §, which was enacted in 1917 as part of the Espionage Act, the first statutory pronouncement of general procedures governing the conduct of federal officers during criminal search and seizures. One stated purpose of the Act was to “better [] enforce the criminal laws of the United States.” Pub. L. No. 65-24, 40 Stat. 229. Case law from that period recognized that the Act codified Fourth Amendment guarantees intended to protect against abuse of process and unjustified intrusions on privacy. *See Byars v. United States*, 273 U.S. 28 (1927).

Four years later, the National Prohibition Act of 1923 incorporated by reference the search warrant provisions of the Espionage Act, which provided that warrants could be entrusted only to “civil officer[s] of the United States. ... one ‘duly authorized to enforce or assist in enforcing any law of the United States.’” *Steele v. United States*, 267 U.S. 505, 507 (1925), citing to Volstead Act, 41 Stat. 305, 308. The Fourth Amendment inherently and historically incorporates the notion of accountability. Under the common law, unlawfully obtained evidence may have been admissible at trial, but law enforcement officials faced civil penalties for the improper seizure of such evidence. *See Olmstead v. United*

States, 277 U.S. 438, 462-63 (1928); *Weeks*, 232 U.S. at 390 (“The sheriff must be furnished with a warrant, and take great care lest he commit a trespass”). Initially, federal officers who could authorize and serve warrants were bonded to cover any potential liability. *See Keehn v. United States*, 300 F. 493, 503 (1st Cir. 1924). Under the National Prohibition Act, an officer’s failure to comply with the laws and limitations of a warrant resulted in heavy penalties. 42 Stat. 222, 223-24 (1924).

Guarantees of trustworthiness and accountability under the Fourth Amendment still require zealous protection. As the Supreme Court recently noted, “[t]he value judgment that [has historically] motivated a united democratic people fighting to defend those very freedoms from totalitarian attack is unchanged.” *Watchtower Bible and Tract Soc’y of N.Y., Inc. v. Vill. of Stratton*, 122 S. Ct. 2080, 2091 (2002). Procedural formalities are critical in preserving our privacy in order to maintain cherished values of humanity and civil liberty. In *McVeigh v. Cohen*, 983 F. Supp. 215, 220 (D.D.C. 1998), addressing unauthorized access to electronic communications, the court stated:

In these days of “big brother,” where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed.

983 F. Supp. at 220. Fundamental principles “established by years of endeavor and suffering” cannot be sacrificed to the needs or convenience of law enforcement.

Weeks, 232 U.S. at 393.

II. Section 3105 Requires the Presence of a Police Officer During the Service of a Warrant and This Circuit has Made Clear that State Officers Must Comply With the Statutory Obligation

Because the search warrant in this case was served in violation of the plain language of § 3105, this court must uphold the determination of the district court that the search was improper. Section 3105, which dictates the procedure for service of a search warrant, provides:

A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such a warrant, but no other person, except in aid of the officer on his requiring it, he being present and acting in its execution.

18 U.S.C. § 3105. The plain language of the statute dictates that search warrants are to be served by an authorized law enforcement officer and no other person.

This statutory safeguard codifies centuries of common law mandating police presence during the exercise of Fourth Amendment authority.

The government argues that § 3105 does not apply when state officers serve and execute a state search warrant. Brief of Appellant, at 10-12. However, the Supreme Court has stated unambiguously that federal law governs the use of evidence in a federal prosecution, even if the evidence was collected by state officers acting pursuant to a state warrant. *Elkins v. United States*, 364 U.S. 206,

224 (1960) (holding that in determining whether there has been an unreasonable search and seizure by state officers, a federal court should apply federal law).

Consistent with that authority, this circuit evaluates challenges to a search conducted by state authorities under federal Fourth Amendment standards. *See United States v. Bieri*, 21 F.3d 811, 816 (8th Cir. 1994) (“[a] court must examine the legality of a search by state officers as if made by federal officers.”).

Contrary to the government's assertion, the authority it cites provides only that 18 U.S.C. § 3109—not § 3105—does not apply to searches where there are exigent circumstances and no significant federal officer involvement. *United States v. Murphy*, 69 F.3d 237, 242 (8th Cir. 1995); *see also United States v. Appelquist*, 145 F.3d 976 (8th Cir. 1998); *United States v. Moore*, 956 F.2d 843, 846 (8th Cir. 1992). In any event, these cases relate to the exigent circumstances exception to application of Fourth Amendment warrant requirements. *Murphy*, 69 F.3d at 242.

Where exigent circumstances exist—such as danger to officers or others, or an imminent threat that evidence will be destroyed—police are not required to “knock and announce” during a search, which enables officers to protect lives, property, and evidence. *United States v. Ramirez*, 523 U.S. 65, 70 (1998); *see also 2 LaFare, Search & Seizure* § 4.8(a), 599-600 (3d ed. 1996). Clearly, the exigent circumstances exception simply does not apply to this case. The police officers in *Murphy* believed that their safety would be at risk if they were required to follow

procedural safeguards, such as knocking at the door, when searching the home of a man who possessed firearms and had a history of violence. 69 F.3d at 243. Only those exigent circumstances justified the officers following a more relaxed procedure than required by § 3109. *Id.*

There are no exigent circumstances present in this case—nor, indeed, has the government argued that an exigent circumstance exception should apply. The police were pursuing a routine investigation involving the service of a warrant on an ISP. Therefore, the fact that § 3109 may not apply to state searches where there are exigent circumstances and no significant federal involvement is not relevant here, where the application of § 3105 is at issue. Thus, unlike in *Murphy*, this case contains no justification for relaxing search warrant service standards.

III. The Fourth Amendment Requires that A Law Enforcement Officer Personally Serve A Warrant For A Search of An E-Mail Service Provider's Remotely Stored Files.

A. Law Enforcement Officers Must Observe Fourth Amendment Procedures to Secure the Privacy Interests of Internet Users.

Fourth Amendment protections must be secured to protect users of the Internet. It is well established that an individual is afforded Fourth Amendment protection against search and seizure when 1) the individual displays a subjective expectation of privacy, and 2) this expectation is one that society would view as reasonable. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J.,

concurring); *see also* *Kyllo v. United States*, 533 U.S. 27, 33 (2001); *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979).

The government tacitly concedes that individuals have a reasonable expectation of privacy in e-mail transmitted by an ISP.³ Indeed, it would be disingenuous for the government to assert otherwise, as it sought and obtained a

³ Courts reviewing the issue have determined that individuals have an expectation of privacy in the contents of their email account. *See United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996). Fourth Amendment protections arise when an individual demonstrates an expectation of privacy in the property to be searched. *Katz*, 389 U.S. at 361. Society would readily recognize as reasonable a user's expectation that the contents of an account maintained with an e-mail provider are private because the average Internet user does not understand the technical processes by which information is transmitted over the Internet. Indeed, e-mail providers such as Yahoo! foster this sense of security.

When a subscriber opens an account with an e-mail provider such as Yahoo!, he or she is repeatedly assured by the provider that the contents of that account are private. For example, Yahoo! draws a distinction between "publicly accessible" areas of Yahoo!, which are "areas of the Yahoo network properties that are intended by Yahoo to be available to the general public," and "services intended for private communication," such as Yahoo!'s e-mail and instant messenger services. Yahoo! Terms of Service, <http://docs.yahoo.com/info/terms> (last accessed July 26, 2002). Yahoo! E-mail accounts are password protected, and Yahoo! explains that mail is not accessible without an account name and password. Yahoo! Online Support at [http:// help.yahoo.com/help/us/mail/access/access-09.html](http://help.yahoo.com/help/us/mail/access/access-09.html) (last accessed July 26, 2002). In its Privacy Policy, Yahoo! explains that even personal non-content information, in which courts have held users have no reasonable expectation of privacy, will be disclosed to law enforcement officers only pursuant to "subpoenas, court orders, or legal process[.]" Yahoo! Privacy Policy at <http://privacy.yahoo.com> (last accessed July 26, 2002). In addition, Yahoo!'s Terms of Service explicitly assure users that Yahoo! only releases content information subject to validly exercised law enforcement procedures. <http://docs.yahoo.com/info/terms>. For these reasons, a subscriber of an e-mail provider would reasonably believe that messages contained in his e-mail account are private.

search warrant to procure the e-mails sought in this case. A search warrant—which requires a showing of probable cause—regulates government access to places and things protected by the Fourth Amendment.

Once Fourth Amendment protection attaches, it “protects people, not places.” *Katz*. at 351. This distinction is particularly relevant to privacy interests concerning the Internet, which is not a physical place; therefore, searches for electronic material must respect the privacy of the individual who composed or received the electronic material.

The application of Fourth Amendment protection to privacy interests in digital environments raises important questions concerning the procedural service of a valid search warrant. As the legal system responds to advances in technology—particularly in the context of electronic communications—the law must protect Fourth Amendment guarantees by ensuring that searches are conducted in a manner conducive to the preservation of privacy interests. As one commentator has noted:

Communication in cyberspace must be protected to the same extent as is more traditional communication if our advancing communication technology is to achieve its full potential without the sacrifice of any of the free speech or privacy that we enjoy today.

Note: Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication, 110 Harv. L. Rev. 1591,1608 (1997).

B. Because An E-Mail Provider Is Immune from Liability Stemming from Its Cooperation with A Warranted Search, It Is Imperative To Foster Accountability By Preserving The Formalities Associated with Service of A Search Warrant.

The government would like to seize information in which individuals have a constitutionally protected expectation of privacy merely by turning on a fax machine. This is simply not an acceptable means of intruding into the privacy interests of the millions of citizens who, increasingly, are transmitting the most personal and intimate details of their lives via the Internet.

To determine the constitutional validity of a search, the court must examine the “totality of the circumstances,” to decide whether the search was reasonable in light of Fourth Amendment guarantees. *Ohio v. Rubinette*, 519 U.S. 33, 39 (1996). The reasonableness of a search is measured "by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *United States v. Knights*, 122 S. Ct. 587, 591 (2001) (*quoting Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). The Fourth Amendment prohibits every search that is unreasonable, and is construed broadly by courts to secure rights of privacy. *United States v. Lefkowitz*, 285 U.S. 452, 464 (1932). Under this standard, the Fourth Amendment requires a law officer personally to serve a warrant to commence the search of an ISP’s e-mail records, even though the officer does not personally need to conduct the search.

Law enforcement officers are legally obligated to ensure Constitutionally protected the privacy rights of citizens. An officer, by virtue of his or her vocation, has knowledge and experience regarding the legality of the scope of a search that a civilian aiding in the search does not, even if the civilian is an expert in the technical methods by which the search is conducted.⁴

The Department of Justice, in guidance it distributes to prosecutors and investigators, assumes the physical presence of police officers for the execution of a warrant on an ISP. *See* U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 51-52 (March 2001). It envisions that the responsibility of one member of the search team

⁴ The extent to which an officer relies upon the aid of a third party during a warranted search will, of course, vary with the circumstances of each case. *See Massachusetts v. Sbordone*, 424 Mass. 802, 809 (Mass. 1997); *Washington v. Kern*, 81 Wash. App. 308, 914 P.2d 114 (Wash. App. 1996). Particularly in searches of digital information, the method by which the search must be conducted may exceed the scope of an officer's technical expertise. *See United States v. Schwimmer*, F. Supp. 119, 126-127 (E.D.N.Y. 1988). However, an officer's physical presence during the service of a warrant, no matter how formal, is never superfluous. Rather, it is a critical safeguard of the rights of the subject of the search:

[a law enforcement officer's] oath of is no small moment as a protection to our citizens when their privacy is lawfully intruded upon by a search pursuant to a warrant . . . it is of great importance that the police authorized to conduct the search do so. They are especially charged and trained to see that the search is carried out properly, lawfully, and in accord with the provisions of the warrant.

Morris v. Florida, 622 So.2d 67, 69 (Fla. App. 1993).

present on the scene is to "review[] the . . . warrant and make[] sure that the entire process complies with the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure." *Id.* at 52.

ISPs, on the other hand, are bound by no such professional or legal concern and are in fact expressly exempt from any liability arising from their participation in a warranted search. 18 U.S.C. § 2703(e). For this reason, a provider has no particular incentive to conduct a search cautiously and deliberately, with due consideration for an individual's privacy rights. If, however, an officer permits a violation of an individual's constitutionally protected interests during a warranted search, the items seized will be excluded from use in any subsequent prosecution. Therefore, an officer's presence during the service of a warrant is an important preliminary safeguard to ensure that a warrant is not executed in a manner that infringes upon an individual's Fourth Amendment rights, even if the officer does not actually conduct the search. The electronic medium searched may be unfamiliar to an officer, but the procedures used to carry out a warranted search remain the same. There is no reason to stray from the tried-and-true formalities that dictate the service and execution of warrants in more traditional situations.

The preservation of Fourth Amendment privacy rights far outweighs either the relatively marginal inconvenience to service providers that must tolerate the presence of an officer who serves a warrant, or the minor inconvenience to officers

when they are required to be present. In "traditional" searches, the inconvenience suffered by officers and by third parties whose premises have been searched has not proven so burdensome as to disrupt daily business or cause serious financial detriment to those involved. There is no reason why personal service of a warrant incident to the search of remote provider files should present a different scenario. If the government seeks to search an individual's property, it must ensure the presence of a law enforcement officer to personally serve the warrant, to ensure that the search is no more invasive than absolutely necessary.

CONCLUSION

Congress and the courts have long recognized a need to safeguard Fourth Amendment privacy guarantees by requiring officers to observe certain formalities during the service of a search warrant. 18 U.S.C. § 3105 codifies the performance of a critical component of these formalities, and should govern searches conducted in digital environments. Internet users have a Fourth Amendment privacy right in digital information remotely stored by ISPs, and the intangible nature of the medium does not in any way compromise or invalidate Internet users' constitutional rights. For this reason, this Court should affirm the judgment of the district court below.

CERTIFICATE OF COMPLIANCE

The undersigned attorney for the *Amicus Curiae* certifies that this brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32. This brief contains 3,493 words, and therefore complies with the 7000-word limit imposed upon *amicus curiae* briefs by Fed. R. App. P. 29(d) and Fed. R. App. P. 32(a)(7)(i). This brief was prepared using Microsoft Word 97/98.

Respectfully submitted,

MARC ROTENBERG
MIKAL CONDON
ELECTRONIC PRIVACY INFORMATION
CENTER
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for *Amicus Curiae*

Marcia Hofmann
Carla Meninsky
Dwayne Nelson

Law Clerks

CERTIFICATE OF SERVICE

I hereby certify that on this 26th day of July, 2002, two copies of the foregoing Amicus Brief of the Electronic Privacy Information Center were served on the following by first-class U.S. mail: Bridgid E. Dowdal, Esq., Paul H. Luehr, Esq., William M. Orth, Esq.

Mikal Condon