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 *Amici Curiae* Yahoo!, Inc., the Computer & Communications Industry Association, NetCoalition and the United States Internet Service Providers Association In Support of Appellant United States of America and Urging Reversal

---

Jonathan Band
Lois K. Perrin
MORRISON & FOERSTER LLP
2000 Pennsylvania Avenue, N.W.
Suite 5500
Washington, D.C. 20006
(202) 887-1500

Attorneys for *Amici Curiae*

CORPORATE DISCLOSURE STATEMENT OF AMICI

1. Pursuant to Fed. R. App. P. 26.1 and Eighth Circuit Rule 26.1A, *amicus* Yahoo!, Inc. states that it has no parent corporation and further that Softbank America, Inc. owns more than ten percent (10%) or more of Yahoo!, Inc.'s stock. Softbank America, Inc. is a wholly owned subsidiary of Softbank Holdings, Inc., which, in turn, is wholly owned by Softbank Corporation.

2. Pursuant to Fed. R. App. P. 26.1 and Eighth Circuit Rule 26.1A, *amicus*, the Computer & Communications Industry Association (CCIA) states that it is a non-profit trade association and as such has no parent corporation nor any issued stock or partnership shares.

CCIA's members include: AOL Time Warner; Atreus Corporation; Block Financial Corporation; CAI/SISCo; Datum, Inc.; Eastman Kodak Co.; Entegrity Solutions Corporation; Fujitsu Limited; Giga Information Group; Government Sales Consultants, Inc.; Hitachi Data Systems, Inc.; Intuit, Inc.; Merant; NetCom Solutions International, Inc.; NOKIA; Nortel Networks; Novak Biddle Venture Partners; NTT America, Inc.; Okidata; Oracle Corporation; QuickHire; SABRE Inc./Travelocity; Sun Microsystems, Inc.; Tantivy Communications, Inc.; Time Domain Corporation; United Parcel

Service; Valaran Corporation; Verio, Inc.; Verizon; ViON Corporation; Yahoo!, Inc.; and YourDictionary.com.

3. Pursuant to Fed. R. App. P. 26.1 and Eighth Circuit Rule 26.1A, *amicus* NetCoalition states that it is a non-profit trade association and as such has no parent corporation nor any issued stock or partnership shares.

NetCoalition's members include: AOL Time Warner, Doubleclick, Inktomi, Terra Lycos, Verio and Yahoo!, Inc.

4. Pursuant to Fed. R. App. P. 26.1 and Eighth Circuit Rule 26.1A, *amicus* United States Internet Service Providers Association (USISPA) states that it is a non-profit trade association and as such has no parent corporation nor any issued stock or partnership shares.

USISPA's members include: AOL Time Warner; Cable & Wireless; eBay; Earthlink; BCE Teleglobe; Verizon; and WorldCom.

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT OF AMICI i

TABLE OF AUTHORITIES iv

INTERESTS OF AMICI 1

ARGUMENT 4

I. REQUIRING THE PHYSICAL PRESENCE OF LAW ENFORCEMENT OFFICERS DURING THE SERVICE AND EXECUTION OF A SEARCH WARRANT ON AN INTERNET SERVICE PROVIDER IS NEITHER REQUIRED BY NOR WILL IT WILL FURTHER THE OBJECTIVES OF THE FOURTH AMENDMENT. 5

II. REQUIRING THE PHYSICAL PRESENCE OF LAW ENFORCEMENT OFFICERS DURING THE EXECUTION OF A SEARCH WARRANT ON AN INTERNET SERVICE PROVIDER WILL PLACE A HEAVY BURDEN ON SERVICE PROVIDERS 10

III. CONCLUSION 13

TABLE OF AUTHORITIES

CASES

Application of the United States for an Order Authorizing the Installation of a Pen Register or Touch-Tone Decoder and Terminating Trap, Bell Telephone Co. of Pennsylvania, 610 F.2d 1148 (3rd Cir. 1979) 6

Baggett v. Bullitt, 377 U.S. 360 (1964) 13

Baird v. State Bar of Arizona, 401 U.S. 1 (1971) 13

In re Application of the United States for an Order Authorizing an In-Progress Trace of Wire Communications Over Telephone Facilities, United States v. Mountain States Telephone & Telegraph Co., 616 F.2d 1122 (9th Cir. 1980) 6

Keyishian v. Board of Regents, 385 U.S. 589 (1967) 13

Laird v. Tatum, 408 U.S. 1 (1972) 13

Lamont v. Postmaster General, 381 U.S. 301 (1965) 13

Ohio v. Robinette, 519 U.S. 33 (1996) 6

Schalk v. Texas, 767 S.W.2d 441 (Tex. App. 1988) 8

United States v. Bach, Crim. File No. 01-221, 2001 U.S. Dist. LEXIS 21853 (December 14, 2001) 5, 7

Wilson v. Arkansas,
514 U.S. 927 (1995) 6

CONSTITUTION

U.S. Const. Amend. IV 4

OTHER AUTHORITIES

Fed. R. App. P. 26.1 ..... i, ii

Fed. R. App. P. 29(b) 3

Eighth Circuit Rule 26.1A ..... i, ii

INTERESTS OF *AMICI*

Yahoo!, Inc. (Yahoo!) is a global Internet communications, commerce and media company that offers a comprehensive branded network of services to more than 219 million individuals each month worldwide. Yahoo! provides communications services such as email, clubs, and chatrooms. It offers commerce services such as online auctions and stores. Yahoo! was the email service provider that received the search warrant at issue in this case.

The Computer & Communications Industry Association (CCIA) is an association of computer, communications, Internet and technology companies that range from small entrepreneurial firms to some of the largest members of the industry. CCIA's members include equipment manufacturers, software developers, providers of electronic commerce, networking, telecommunications and online services, resellers, systems integrators, and third-party vendors.[1] Its member companies employ nearly

[1] CCIA's members include: AOL Time Warner; Atreus Corporation; Block Financial Corporation; CAI/SISCo; Datum, Inc.; Eastman Kodak Co.; Entegrity Solutions Corporation; Fujitsu Limited; Giga Information Group; Government Sales Consultants, Inc.; Hitachi Data Systems, Inc.; Intuit, Inc.; Merant; NetCom Solutions International, Inc.; NOKIA; Nortel Networks; Novak Biddle Venture Partners; NTT America, Inc.; Okidata; Oracle Corporation; QuickHire; SABRE Inc./Travelocity; Sun Microsystems, Inc.; Tantivy Communications, Inc.; Time Domain Corporation; United Parcel

one million persons and generate annual revenues exceeding $300 billion. CCIA's mission is to further the interests of its members, their customers, and the industry at large by serving as the leading industry advocate in promoting open, barrier-free competition in the offering of computer and communications products and services worldwide.

NetCoalition serves as the public policy voice for some of the world's most innovative Internet companies on the key legislative and administrative proposals affecting the online world.[2] A respected resource, NetCoalition provides creative and effective solutions to the critical legal and technological issues facing the Internet. By enabling industry leaders, policymakers, and the public to engage directly, NetCoalition has helped ensure the integrity, usefulness, and continued expansion of this dynamic new medium.

The United States Internet Service Provider Association (USISPA) is a trade association that represents the interests of major Internet Service

---

Service; Valaran Corporation; Verio, Inc.; Verizon; ViON Corporation; Yahoo!; and YourDictionary.com.

[2] Members of NetCoalition include AOL Time Warner, Doubleclick, Inktomi, Terra Lycos, Verio and Yahoo!.

Providers. USISPA's members provide a range of Internet services to citizens and businesses.[3]

The physical presence rule established by the court below, if followed nationwide, would place significant burdens on *amici* and similarly situated service providers. At any one time, conceivably dozens of law enforcement officers would be on the premises of any given service provider, waiting for its employees to retrieve the information specified in the warrants served. This law enforcement presence would be disruptive and intimidating to the service provider's employees. Additionally, this regular on-site law enforcement presence would threaten the privacy of the service provider's subscribers and chill their freedom of speech.

This significant burden on service providers is not offset by a meaningful increase in protection of the Fourth Amendment rights of the targets of criminal investigations. To the contrary, the physical presence rule could actually diminish the protections afforded the suspects — who are our subscribers. Accordingly, *amici* have a great interest in seeing the ruling below reversed.

Filed concurrently with this brief pursuant to Fed. R. App. P. 29(b) is a Motion for Leave to File Brief of *Amici Curiae* Yahoo!, CCIA,

[3] Members of the USISPA include: AOL Time Warner; Cable & Wireless;

NetCoalition and USISPA Supporting Appellant United States and Urging Reversal.[4]

ARGUMENT

The court below ruled that an Internet service provider's retrieval of information in response to a faxed search warrant was an unreasonable search and seizure in violation of the Fourth Amendment. U.S. Const. Amend. IV. The court did not object to the service provider's rendering of assistance to law enforcement; rather, the court objected to the rendering of assistance outside the physical presence of a law enforcement officer. The court found that without the police officer's supervision and instruction, the service provider's search could exceed the bounds of the warrant. However, because of the technological difficulty of locating and retrieving information from a service provider's advanced computer networks and data warehouses, the police officer cannot effectively supervise a search conducted by the service provider's employees. Thus, the officer's physical presence will not safeguard a suspect's rights by keeping the search limited.

At the same time, a physical presence requirement will disrupt the efficient operation of a service provider's business. In sum, the ruling

---

eBay; Earthlink; BCE Teleglobe; Verizon; and WorldCom.

[4] Appellant United States of America consented to the filing of this brief, but Appellee Dale Richard Bach withheld consent.

below fails to protect criminal suspects from unreasonable searches and seizures, while simultaneously imposing an unreasonable burden on service providers and their subscribers.

I. REQUIRING THE PHYSICAL PRESENCE OF LAW ENFORCEMENT OFFICERS DURING THE SERVICE AND EXECUTION OF A SEARCH WARRANT ON AN INTERNET SERVICE PROVIDER IS NEITHER REQUIRED BY NOR WILL IT WILL FURTHER THE OBJECTIVES OF THE FOURTH AMENDMENT.

The court below asserts that "the requirement that an officer be present and acting in a warrant's execution when a third party is assisting the officer helps to effectuate the fundamental Fourth Amendment protection against general searches and seizures." *United States v. Bach*, Crim. File No. 01-221, 2001 U.S. Dist. LEXIS 21853 at *8 (December 14, 2001). The court explains that the officer can supervise and instruct the civilian employees: "Police officers have taken an oath to uphold federal and state Constitutions and are trained to conduct a search lawfully and in accordance with the provisions of a warrant." *Id*. at *9. The court states that the officer acts as a "safeguard" to ensure that a service provider does not "traverse the clearly defined limits of a warrant." *Id*.

The stringent physical presence rule articulated and applied by the court below is simply not mandated by the Fourth Amendment. Indeed, as the United States Supreme Court has stated, the standard for evaluating

conduct for compliance with the Fourth Amendment is one of reasonableness. *See, e.g., Ohio v. Robinette*, 519 U.S. 33, 39 (1996); *Wilson v. Arkansas*, 514 U.S. 927, 934 (1995). The lower court's rule, while perhaps reasonable with respect to traditional searches conducted by third party civilians, is completely unreasonable with respect to searches of the electronic records of Internet service providers. The information sought from Internet service providers is stored on computer servers that typically are configured to maximize the speed and efficiency of the service, rather than to facilitate the retrieval of the information by human beings. This configuration often requires that the searches be conducted by highly skilled technicians. Indeed, some searches are so complex they must be performed by engineers with degrees in computer science.[5] Every Internet service provider configures its computer systems in a different way, and often has

[5] At least two courts of appeals have recognized that the emergence of new technologies may create situations in which civilian technicians are often the only persons with the requisite expertise to perform the searches and are therefore necessary to assist the police in executing a warrant. *See Application of the United States for an Order Authorizing the Installation of a Pen Register or Touch-Tone Decoder and Terminating Trap, Bell Telephone Co. of Pennsylvania*, 610 F.2d 1148 (3rd Cir. 1979); *In re Application of the United States for an Order Authorizing an In-Progress Trace of Wire Communications Over Telephone Facilities, United States v. Mountain States Telephone & Telegraph Co.*, 616 F.2d 1122 (9th Cir. 1980). In each of these cases, which involved challenges to the then novel technology used to trace phone numbers, the courts of appeals expressly rejected the physical presence requirement. *Ibid.*

different structures for different services — *e.g.*, email vs. clubs vs. bulletin boards. A large service provider may offer close to 100 different services, which can translate into 100 different ways information is stored and thus 100 different ways information must be retrieved.

Thus, although a police officer may well be "trained to conduct a search lawfully and in accordance with the provisions of a warrant," she is not trained to conduct an effective search of the computer systems of an Internet service provider. *U.S. v. Bach* at *9. She is in no position to supervise or instruct the service provider's technicians as they search for the information requested in the warrant; they must conduct the search themselves, from their computer terminals. The police officer waiting in the lobby while the technician works away on the computer does not in any way safeguard anyone's Fourth Amendment rights.

Conceivably the police officer could sit next to the technician as the technician retrieved the requested information. But this would increase, rather than decrease, the likelihood of an overly broad search. For example, a technician might have to retrieve all of the emails sent by an individual before the technician isolates the email that falls within the specific date range covered by the warrant. By sitting next to the technician, the police officer might see the subject lines or addressees of some of the emails

outside the warrant's date range before the engineer manages to isolate the responsive email. Similarly, the police officer might see the user names and passwords the technician uses to access the information. This could compromise the security of the service provider's system, and lead to abuses of the Fourth Amendment rights of millions of subscribers.

Even if a police officer had some relevant technical training, the officer would not be familiar with a particular service provider's system. As a result, the officer would not have the expertise to perform a search in the most effective way to limit the information collected to only that requested by the warrant. The officer would be exposed to non-responsive information. Moreover, in the highly unlikely event that the officer was familiar with the specific system, the officer probably would still see information outside the scope of the warrant. Information typically cannot be retrieved in tidy bundles precisely responsive to a warrant's request; culling and redacting is almost always necessary.

The compliance system large service providers have in place is far more likely to safeguard subscribers' rights than police presence. *See Schalk v. Texas*, 767 S.W.2d 441, 454 (Tex. App. 1988) *aff'd*, 823 S.W.2d 633 (Tex. Crim. App. 1991) (civilian assistance "would tend to limit or restrict the items seized rather than enlarge upon them"). Large service providers

typically have a compliance team supervised by the General Counsel's office. When a warrant is received, a member of the compliance team works with the technicians with the proper expertise to retrieve the kind of data requested. The compliance team member reviews the material gathered by the technicians, determines what is responsive to the warrant, and turns that material over to the law enforcement authorities. Some service providers have this review performed by an attorney.

The vast majority of Internet services are rendered by large service providers, meaning that the vast majority of warrants are processed in the manner described above. But even with warrants directed to small service providers that do not have a compliance team, the physical presence of an officer will not safeguard a suspect's Fourth Amendment rights. The search will still need to be performed by a technician whom the officer is not capable of supervising or instructing. Requiring the physical presence of an officer while a large or small Internet service provider is responding to a search warrant would be a triumph of form over substance.

There is an illogic at the heart of the decision below. Putting aside the unique Internet context at issue in this case, as a general matter it is true that a properly supervised civilian would be less likely to go beyond the scope of a warrant than an unsupervised civilian. But so what? If the unsupervised

civilian produces too much information, the officer is free to discard it or return it to the civilian's employer. Why is this any worse than the officer conducting the search herself, and culling through a mass of information to identify responsive material? The rights of the suspect — and others — are always more secure when a civilian, either supervised or unsupervised, makes a "first cut" of the information than if the police officer performs the search herself. When a civilian makes a first cut, the universe of nonresponsive information that the officer sees is far smaller than if the officer performs the initial search. In short, the physical presence rule arguably makes no sense in any context.

II. REQUIRING THE PHYSICAL PRESENCE OF LAW ENFORCEMENT OFFICERS DURING THE EXECUTION OF A SEARCH WARRANT ON AN INTERNET SERVICE PROVIDER WILL PLACE A HEAVY BURDEN ON SERVICE PROVIDERS.

The United States in its brief describes the heavy burden the ruling below will place on law enforcement. *See* Appellant's Brief at 20-22. The ruling below will also place a significant burden on Internet service providers.

A large Internet service provider can receive literally thousands of search warrants and other requests for information during the course of a year. Since September 11, 2001, the volume of warrants has increased. The

volume likely will increase even more when the Council of Europe Cybercrime Convention, an international treaty with mutual assistance provisions that require the United States to obtain information from Internet service providers at the request of foreign governments, takes effect. The large number of the warrants, and the difficulty of retrieving the responsive information, means that the search often occurs in stages and that several days may elapse between the service of the warrant and the completion of the search. If an officer had to be physically present for this entire period, it is entirely possible that at any given time a dozen or more law enforcement officers would be on the premises of a given service provider.

While some employees might find this large law enforcement presence comforting, others might find it threatening. However, all employees would find it disruptive. The disruption probably would be greatest if the officers sat next to the technicians as they searched for information. But disruption would also result from a large number of officers sitting in a reception area of a firm designed to conduct business online rather than in person.

A physical presence requirement would also disrupt the orderly processing of information requests. Currently, the service providers' compliance officers prioritize information requests based on the urgency of

the request, how long it will take to retrieve the information, the work schedule of the technicians, and related considerations. A physical presence requirement would cause the compliance officers to place the warrants ahead of all other information requests (such as grand jury subpoenas or civil discovery) in the interest of getting the law enforcement officers off the premises as quickly as possible. This disruption of the sequence of searches might prevent the searches from being conducted at optimal times, such as during the early morning hours when network demand is lowest.

A physical presence requirement would be burdensome even if the officer had to be present only when the service provider took action on the warrant. An officer might serve a warrant at 10:00 a.m.; the compliance officer might review the warrant and assign it to a technician at 2:00 p.m.; the technician might retrieve some of the information from a server at 10:00 p.m., and other information from a back-up tape at 10:00 p.m. the next evening; and the compliance officer might redact the information so that it does not exceed the scope of the warrant on 10:00 a.m. of the third day. For the officer to be present whenever action was taken on the warrant, the service provider would have to establish and keep to a schedule, and hope that the officer was present when necessary. Further complicating this scheduling is that some of the requested information may be stored at a

remote location and might perhaps be retrievable only by technicians working at that location. Under the lower court's rule, a police officer presumably would have to be physically present at the remote location when the technician conducted the search there.

Finally, once the regular physical presence of officers at service providers was known in the Internet community, subscribers understandably would become concerned about the privacy and security of their online communications. This could chill their freedom of speech. The United States Supreme Court has found "in a number of cases that constitutional violations may arise from the deterrent, or 'chilling,' effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights." *Laird v. Tatum*, 408 U.S. 1 (1972); *see also Baird v. State Bar of Arizona*, 401 U.S. 1 (1971); *Keyishian v. Board of Regents*, 385 U.S. 589 (1967); *Lamont v. Postmaster General*, 381 U.S. 301 (1965); *Baggett v. Bullitt*, 377 U.S. 360 (1964). These privacy and security concerns could diminish Internet usage which, in turn, could harm the finances of Internet service providers.

III. CONCLUSION

In an effort to ensure that searches and seizures of information held by Internet service providers were reasonable under the Fourth Amendment, the

court below fashioned a rule that is completely unreasonable. Requiring the physical presence of an officer during a search does not safeguard a suspect's rights; to the contrary, it threatens the privacy rights of the service provider's subscribers. Additionally, the physical presence rule imposes a significant burden on the service provider, as well as law enforcement authorities at all levels. In short, the physical presence rule imposes many costs but no benefits. This Court should reverse the ruling of the district court.

May 13, 2002

Respectfully submitted,

_____

Jonathan Band
Lois K. Perrin
Morrison & Foerster LLP
2000 Pennsylvania Ave., NW,
Suite 5500
Washington, D.C., 20006
(202) 887-1500

Counsel for *Amici Curiae*

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C) and Eighth Circuit Rule 28 (A)(c) and (d), I hereby certify that this brief was prepared in Microsoft Word 1997 and that it uses a 14 point proportional type font "Times New Roman." This brief consists of fewer than 15 pages and is therefore exempt from the volume requirement of Fed. R. App. P. 32(a)(7)(C). *See* Fed. R. App. P. 32(a)(7)(A). Additionally, the diskette that is being filed with this Court and the diskettes that are being served upon counsel for Appellant and Appellee have been scanned for viruses and are virus-free.

May 13, 2002

Jonathan Band
Counsel for Amici Curiae

dc- 310946

CERTIFICATE OF SERVICE

I hereby certify that on this 13th day of May, 2002, an original and nine copies of the preceding Brief of Amici Curiae Yahoo!, Inc., the Computer & Communications Industry Association, NetCoalition and the United States Internet Service Providers Association In Support of Appellant United States of America and Urging Reversal, and a copy of the brief on diskette were served on this Court by placing the same in a box or other facility regularly maintained by UNITED PARCEL SERVICE ("UPS") or delivering the same to an authorized courier or driver authorized by UPS to receive documents on the same date that it is placed at Morrison & Foerster LLP for collection, addressed to:

U.S. COURT OF APPEALS FOR THE EIGHTH CIRCUIT
CLERK'S OFFICE
THOMAS F. EAGLETON COURT HOUSE
ROOM 24.329
111 S. 10TH STREET
ST. LOUIS, MISSOURI 63102

I also certify that, on the same date, two copies of the preceding Brief of Amici Curiae Yahoo!, Inc., the Computer & Communications Industry Association, NetCoalition and the United States Internet Service Providers Association In Support of Appellant United States of America and Urging Reversal, and a copy of the brief on diskette were served on counsel for

Appellant and Appellee by placing the same in a box or other facility regularly maintained by UPS or delivering the same to an authorized courier or driver authorized by UPS to receive documents on the same date that it is placed at Morrison & Foerster LLP for collection, addressed to:

Bridgette E. Dowdal, Esq.
U.S. Attorney's Office
300 S. Fourth Street
600 U.S. Courthouse
Minneapolis, MN 55415
Telephone: (612) 664-5600
Counsel for Appellant United States.

William M. Orth, Esq.
Orth Law Office
247 Third Avenue, S. #100
100 Barristers Trust Building
Minneapolis, MN 55415-1056
Phone: (612) 333-6440
Counsel for Appellee Robert Bach.

May 13, 2002

Jonathan Band
Counsel for Amici Curiae