No. 03-1383

In the United States Court of Appeals for the First Circuit

UNITED STATES OF AMERICA,

Appellant,

v.

BRADFORD C. COUNCILMAN,

Appellee.

On Appeal From the United States District Court
for the District of Massachusetts

Brief on Rehearing En Banc of *Amicus Curiae* Technical Experts in Support of Appellant, Urging Reversal

MARC ROTENBERG
Georgetown University Law Center
600 New Jersey Ave., NW
Washington, DC 20001

MARCIA HOFMANN
2118 18th St. NW
Washington, DC 20009

(affiliations for identification purposes only)

Counsel for *Amicus Curiae*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

United States v. Councilman, 373 F.3d 197, 204 (1st Cir. 2004) 3, 6

OTHER AUTHORITIES

Email communications from Vinton G. Cerf to Marc Rotenberg,
Executive Director, EPIC (Nov. 12, 2004) (on file with EPIC) 7

Bryan Costales and Eric Allman, *Sendmail* (O'Reilly, 2nd ed. 1997) 4

Encyclopedia of Computer Science (Anthony Ralston et al. eds.,
Nature Publishing Group, 4th ed. 2000) 3, 4, 5, 6

Stephen Keeling, *Filtering Mail with Procmail* (last accessed
Nov. 11, 2004) 5

J. Klensin, Internet Engineering Task Force, *RFC 2821 - Simple Mail
Transfer Protocol* (April 2001) 4

C. Partridge, Internet Engineering Task Force, *RFC 974 – Mail Routing
and the Domain System* (Jan. 1986) 4-5

Jonathan B. Postel, Internet Engineering Task Force, *RFC 821 – Simple
Mail Transfer Protocol* (Aug. 1982) 6-7

Robert Ellis Smith, *Ben Franklin's Web Site: Privacy and Curiosity
from Plymouth Rock to the Internet* (Privacy Journal 2000) 8

The Tao of IETF, Internet Engineering Task Force (Aug. 2001) 7

STATEMENT OF *AMICUS CURIAE*

The technical experts participating in this brief are leading authorities on Internet architecture, computer privacy, and email communications. They favor an interpretation of privacy laws that will protect the confidentiality of electronic communications. They are participating in this brief in their individual capacity and not on behalf of any organization or corporation.[1]

Dr. Whitfield Diffie, Chief Security Officer of Sun Microsystems, is the inventor of the concept of public key cryptography which underlies the security of Internet commerce. Since the early 1990s, he has focused on security and technology policy and is the author, along with Susan Landau, of the book *Privacy on the Line: the Politics of Wiretapping and Encryption* (MIT Press 1998).

Dr. Edward W. Felten is a Professor of Computer Science at Princeton University. He has published more than seventy research papers and two books, and he has served as a technical advisor to the U.S. Department of Justice, Department of Defense, and Federal Trade Commission.

Dr. John R. Levine chairs the Internet Research Task Force Anti-Spam Research Group. He is the author of many books on the Internet and electronic mail including *qmail* (O'Reilly, 2004), and *E-mail for Dummies* (IDG

[1] Paul Jones, IPIOP Law Clerk at EPIC, contributed to the preparation of this brief. Kevin Bankston, Chris Palmer, and Seth Schoen of the Electronic Frontier Foundation also assisted.

Books/Wiley, 1997).

Dr. Peter G. Neumann is Principal Scientist in the Computer Science Lab at SRI International, moderator of the ACM Risks Forum (www.risks.org), and author of *Computer-Related Risks* (Addison-Wesley 1994), with a long background in trustworthy systems, security, and privacy.

Dr. Bruce Schneier is Chief Technical Officer of Counterpaine Security. He is the author of many textbooks on computer security and privacy, including *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (Wiley 2003) and *Secrets and Lies: Digital Security in a Networked World* (Wiley 2000).

SUMMARY OF ARGUMENT

Internet-based mail services clearly distinguish between the routine storage that occurs when a message reaches its destination and is available to its intended recipient and the temporary "storage" that occurs as electronic mail moves in many discrete steps from sender to recipient. It is the nature of a "store and forward" communications network that a message would necessarily be accessible at many points in time.

The dissent correctly found that at the time the Electronic Communications Privacy Act was enacted, access to an Internet communication before it was accessible to the intended recipient would be considered an "interception." Any other understanding would render meaningless the distinction between storage and interception for electronic mail that transverses the Internet.

ARGUMENT

The description of electronic mail provided by Judge Lipez in this case accurately describes the nature of Internet-based communications and the need for a strong interpretation of the federal wiretap law. *United States v. Councilman*, 373 F.3d 197, 204 (1st Cir. 2004) (Lipez, J., dissenting). As the judge correctly noted, the technical specifications for electronic mail were first adopted by the group that was coordinating standards for the Internet in 1982, well before the passage of ECPA in 1986.

Our view is that the commonsense understanding of a communication network, both in 1986 when the law was amended and today, is that "storage" occurs only at the endpoint when a message is accessible to the intended recipient.

I. An Email Travels Through a Series of Computers Which Temporarily Hold and Then Forward the Information Before It Reaches Its Final Destination; Any Storage That Occurs is Ephemeral

An email is defined as "the transfer of a message in electronic form from one computer to another, usually over a network." *Encyclopedia of Computer Science* 637 (Anthony Ralston et al. eds., Nature Publishing Group, 4th ed. 2000). Sending an email is analogous in many ways to mailing a letter across the country.

One of a variety of email programs serves as the sender's pen and paper. When the user is ready to send the message, a mail transfer agent ("MTA") analyzes the message to identify the intended recipient. *Id.* at 639.

However, the email need not jump straight from the sender's computer to that of the recipient. A conventional letter sent from New York might travel from one post office to a central sorting station in the East, to another sorting station in the West, to another post office, before being delivered in Los Angeles. Similarly, an email is sent through a series of computers on the network before it reaches its intended addressee. *Id.* at 637. Each of these computers has its own MTA which is responsible for this "hop-to-hop forwarding of messages through the network." *Id.* at 639. Upon receiving an email, each of these computers checks the address of the recipient, and then determines where to send the email next based on its final destination. J. Klensin, Internet Engineering Task Force, *RFC 2821 - Simple Mail Transfer Protocol* (April 2001), *at* http://www.ietf.org/rfc/rfc2821.txt (last accessed Nov. 8, 2004); C. Partridge, Internet Engineering Task Force, *RFC 974 – Mail Routing and the Domain System* (Jan. 1986), *at* http://www.ietf.org/rfc/rfc974.txt (last accessed Nov. 10, 2004). Often, an email cannot be transferred immediately and must be saved for later delivery. Bryan Costales and Eric Allman, *Sendmail* 5 (O'Reilly, 2nd ed. 1997). This process, known as "store and forward," is analogous to a postal carrier attempting to deliver a package only to find that the recipient is not home, and returning later in the day. *Encyclopedia of Computer Science* at 639. Once the email successfully reaches the next leg of its journey, the copy is deleted by the previous computer to make room for new incoming messages. Any storage that occurs during this process is ephemeral.

Eventually the email arrives at the recipient's MTA, which for these purposes is analogous to the hometown post office of the addressee. *Id.* at 637-638. At this point, the message is like a letter sitting in a hopper at the local post office waiting to be delivered. Though it may be stored as part of the process of its delivery, it is still in transmission for all practical purposes because it has not yet been made accessible to its intended recipient.

A mail delivery agent ("MDA") then acts as the postal carrier by determining which user should receive the email and placing the message in that user's mailbox. *Id.* at 638. The MDA is typically controlled by programs called "recipes," which act much like a local postmaster. Stephen Keeling, *Filtering Mail with Procmail, at* http://www.spots.ab.ca/~keeling/procmail.html (last visited Nov. 11, 2004). These files perform a variety of functions, which determine what happens to each email as it is to be delivered to its recipient. *Id.* Recipes can be used to tell the MDA to deposit mail addressed to one address into another user's mailbox, which is similar to conventional mail forwarding. *Id.* For instance, mail sent to "abuse" will be delivered to administrators to determine if someone is using the system for an improper or prohibited purpose.

Finally, the messages are deposited in the addressee's mailbox, and are retrieved and read with an email program. *Encyclopedia of Computer Science* at 638. While this sounds like an involved process, it can all happen in the blink of an eye. Most emails take only a few seconds to complete their journey. Moreover, it was during the extremely short window of time between reception at the final MTA and delivery by the MDA that Councilman was able to intercept, copy and read the correspondence sent to his customers.

Councilman apparently wrote a recipe for his MDA that copied all emails from his competitor, Amazon.com, while the MDA was in the process of placing that message into the recipient's mailbox, and to place these copies into his own personal box. *Councilman*, 373 F.3d at 205 (Lipez, J. dissenting). This is analogous to a postmaster opening and copying all bills and advertisements mailed by Federal Express that pass through his post office.

II. The Development of Electronic Mail Standards Occurred Over a Long Period Prior to Passage of the Electronic Communication Privacy Act

The technical specifications for electronic mail were adopted by the group that was coordinating standards for the Internet in 1982. Jonathan B. Postel, Internet Engineering Task Force, *RFC 821 - Simple Mail Transfer Protocol* (Aug.

1982), *at* http://www.ietf.org/rfc/rfc0821.txt (last accessed Nov. 8, 2004). These standards are maintained and developed by the Internet Engineering Task Force ("IETF"), and embodied in a series of documents called Requests For Comment ("RFCs"). *The Tao of IETF*, Internet Engineering Task Force, (Aug. 2001), *at* http://www.ietf.org/tao.html (last visited Nov. 10, 2004).

According to Internet pioneer Vinton G. Cerf:

> Email was developed for the ARPANET in 1971/1972. RFCs [Request for Comments] documenting the formats and procedures were developed, the key ones being RFC 733, RFC 822 authored in part by David Crocker among others. Email was adapted for Internet use when the Internet was rolled out on the ARPANET starting January 1, 1983. That same year, MCI delivered MCI Mail, a commercial service. Other similar services were offered by CompuServ, Telenet, General Electric Information Services, etc

Email communications from Vinton G. Cerf to Marc Rotenberg (Nov. 12, 2004).

These standards had been implemented and were in common use well before the passage of ECPA in 1986.

III. Privacy is Critical For Electronic Mail, Just As It Is For Mail That Travels by Postal Service

The protection of mail has a long history in the United States because of the obvious concern that a network that fails to safeguard the confidentiality of communications is not useful. In post-colonial America, it was just this fear of a lack of confidentiality that lead those in sensitive positions to shy away from letter writing. Robert Ellis Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* 50 (Privacy Journal 2000). It was generally accepted that postmasters in the late 18th century read the mail that came through their offices. *Id.* at 50. In 1798, then-Vice President Thomas Jefferson noted, "[t]he infidelities of the post office and the circumstances of the times are against my writing fully and freely. I know not which mortifies me most, that I should fear to write what I think, or my country bear such a state of things." *Id.* at 50. To rectify this atmosphere of distrust, Congress required that clerks could not "open, detain, delay, secrete, embezzle, or destroy" any letter without a warrant or the consent of the addressee. *Id.* at 50.

The ECPA was intended to deal precisely with the improper capture of information by one party that is intended solely for delivery to other(s), and the alleged actions by Councilman appear to fit this description.

CONCLUSION

For the foregoing reasons, this Court should reverse the district court's dismissal.

Respectfully submitted,

____
MARC ROTENBERG
Georgetown University Law Center
600 New Jersey Ave., NW
Washington, DC 20001

MARCIA HOFMANN
2118 18th St. NW
Washington, DC 20009

Counsel for *Amicus Curiae*

CERTIFICATE OF SERVICE

I hereby certify that on this 12th day of November, 2004, two copies of the forgoing *amicus curiae* brief were served on the following by First Class U.S. mail:

Joel Gershowitz
John A. Drennan
Appellate Section
Criminal Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Andrew Good, Esq.
Good & Cormier
Attorneys-at-Law
83 Atlantic Avenue
Boston, MA 02110-3711

Orin S. Kerr
George Washington University
Law School
2000 H Street, NW
Washington, DC 20052

____
Marcia Hofmann

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

UNITED STATES OF AMERICA,	)	
	)	No. 03-1383
Appellant,	)	
	)	
v.	)	
	)	
BRADFORD C. COUNCILMAN,	)	
	)	
Appellee.	)	

MOTION OF *AMICUS CURIAE* TECHNICAL EXPERTS FOR LEAVE TO FILE ACCOMPANYING *AMICUS* BRIEF

Pursuant to Fed. R. App. P. 29(b), *amicus curiae* technical experts requests leave to file the accompanying *amicus curiae* brief in support of appellant. This brief urges reversal of the District Court's decision. Only the appellant in this case has consented to the filing of this brief.

The technical experts participating in this brief are leading authorities on Internet architecture, computer privacy, and email communications. In this case, they favor an interpretation of the federal wiretap law that will protect the confidentiality of electronic communications. and therefore respectfully request that this Court grant them leave to file the accompanying *amicus curiae* brief.

Dated: November 12, 2004 Respectfully submitted,

MARC ROTENBERG
Georgetown University Law Center
600 New Jersey Ave., NW
Washington, DC 20001

MARCIA HOFMANN
2118 18th St. NW
Washington, DC 20009

Counsel for *Amicus Curiae*

CERTIFICATE OF SERVICE

I hereby certify that on this 12th day of November, 2004, two copies of the forgoing Motion for Leave to File were served on the following by First Class U.S. mail:

Joel Gershowitz
John A. Drennan
Appellate Section
Criminal Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Andrew Good, Esq.
Good & Cormier
Attorneys-at-Law
83 Atlantic Avenue
Boston, MA 02110-3711

Orin S. Kerr
George Washington University
Law School
2000 H Street, NW
Washington, DC 20052

____
Marcia Hofmann