No. 02-15742

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

GEORGE THEOFEL, et.al.,
Plaintiffs-Appellants,

v.

ALWYN FAREY-JONES, et. al.,
Defendants-Appellees.

On Appeal from the United States District Court
for the Northern District of California

BRIEF FOR THE UNITED STATES AS AMICUS CURIAE SUPPORTING DEFENDANT/APPELLEE'S PETITION FOR REHEARING AND SUGGESTION FOR REHEARING EN BANC

CHRISTOPHER A. WRAY
Assistant Attorney General

MARK ECKENWILER
Deputy Chief
Computer Crime and Intellectual
Property Section

NATHAN JUDISH
Attorney, Computer Crime and
Intellectual Property Section
Criminal Division
U.S. Department of Justice
1301 New York Avenue, NW
Washington, D.C. 20530
(202) 514-1026

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES and RULES

MISCELLANEOUS

INTRODUCTION AND STATEMENT OF INTEREST OF THE UNITED STATES OF AMERICA

The United States of America files this brief pursuant to Fed. R. App. P. 29.

This case, Theofel v. Farey-Jones, No. 02-15742 (9th Cir. Aug. 28, 2003), involves the construction of the term "electronic storage," 18 U.S.C. § 2510(17), which plays a key role in the Stored Communications Act, 18 U.S.C. §§ 2701-2712 ("SCA"). The panel's conclusion — that e-mail messages remain in "electronic storage" regardless of whether they have been accessed by the addressee — is contrary to the SCA's language, structure, and legislative history. Moreover, the panel's unprecedented interpretation of "electronic storage" upends the statutory framework for law enforcement's ability to compel disclosure of stored communications from network service providers, such as ISPs.

The panel's decision in Theofel largely nullifies 18 U.S.C. § 2703(b), the statutory provision of the SCA that governs law enforcement access to electronic communications not in "electronic storage." Federal prosecutors in the Ninth Circuit have ceased using § 2703(b) to compel disclosure of stored communications as a result of Theofel. Moreover, because the Internet spans state and national borders, the panel's decision is likely to create difficulties for law enforcement nationwide. For example, some of the nation's largest e-mail service providers, including Hotmail and Yahoo!, are located in the Ninth Circuit.

Because such service providers must choose between compliance with § 2703(b) process issued elsewhere and adherence to the implications of Theofel, the panel's decision may upset criminal investigations across the United States.

In brief, because the panel's decision in this civil case has enormous implications in criminal law and procedure that the panel apparently did not recognize, the United States respectfully urges the court to grant the Petition for Rehearing and Suggestion for Rehearing En Banc of Defendant/Appellee Alwyn V. H. Farey-Jones (hereinafter "Petition for Rehearing").

STATEMENT OF FACTS

Theofel arose out of a discovery dispute in a separate commercial litigation involving at least two of the plaintiffs in Theofel and defendant Farey-Jones. In this separate litigation, Farey-Jones and his counsel subpoenaed an ISP which provided e-mail service to a corporation associated with the Theofel plaintiffs. The subpoena contained no limits based on time or scope. In response to the subpoena, the ISP copied 339 e-mail messages to a web site, and the messages were reviewed by Farey-Jones and his counsel. A magistrate subsequently quashed the subpoena, finding it "massively overbroad" and "patently unlawful." See Slip op. at 12338-39.

Following the quashing of the subpoena, the plaintiffs (all of whom had their e-mail viewed by the defendants) brought the instant suit seeking damages under the SCA, other federal statutes, and various state laws. Section 2707 of the SCA provides for a civil action against violators of the SCA's provisions. The plaintiffs alleged that the defendants violated § 2701 of the SCA, which provides for criminal penalties for one who "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701. The district court dismissed this claim.

The panel reversed. Only one issue addressed by the panel is of concern to the United States: whether the e-mail messages accessed by the defendants fell outside the scope of § 2701 because they were not "in electronic storage." Although the panel recognized that other courts have limited the definition of "electronic storage" to messages not yet delivered to their intended recipient, it asserted nevertheless that opened e-mails were "for purposes of backup protection" and thus fell within the scope of "electronic storage." Slip op. at 12345. The panel stated that "[a]n obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs

to download it again–if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a 'backup' for the user." Id. The panel concluded that "plaintiffs' e-mail messages were in electronic storage regardless of whether they had been previously delivered." Id. at 12346.

SUMMARY

The Stored Communications Act, 18 U.S.C. §§ 2701-2712, sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers. There are three main substantive components to this system, which serves to protect and regulate the privacy interests of network users with respect to government, network service providers, and the world at large. First, § 2703 regulates government access to stored communications. It creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications. Second, § 2702 regulates voluntary disclosure by network service providers of customer communications and records, both to government and non-governmental entities. Third, § 2701 prohibits unlawful access to certain stored communications; anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties.

The structures of all three substantive components of the SCA reflect a series

of classifications indicating congressional judgments about what kinds of information implicate greater or lesser privacy interests. In general, the SCA offers greater privacy protection to categories of information perceived by the SCA's drafters to implicate greater privacy interests. In setting forth this series of classifications, the SCA relies on a few key terms which are explicitly defined by statute. These terms are used throughout the SCA; a court's interpretation of a term for purposes of one provision of the SCA has important ramifications for the SCA's other provisions. One such term is "electronic storage," defined by 18 U.S.C. § 2510(17). The United States' interest in Theofel is limited to the interpretation of the scope of "electronic storage."

The panel's interpretation of "electronic storage" ignores the plain language of the term's definition, in particular that the "backup" subsection § 2510(17)(B) refers to backups of "temporary, intermediate" communications protected by § 2510(17)(A). The panel also ignored legislative history confirming this interpretation. Moreover, the panel's interpretation upsets the structure of the SCA, including the balance between § 2703(a) and § 2703(b), and in the process creates an unprecedented impediment for law enforcement access to stored communications. Because of the importance of this result for criminal investigations nationwide, the court should grant the Petition for Rehearing.

ARGUMENT

I. THE PANEL'S DECISION MISREADS THE DEFINITION OF "ELECTRONIC STORAGE" AND RENDERS SUPERFLUOUS KEY PORTIONS OF THE STORED COMMUNICATIONS ACT

A. The Panel's Interpretation of "Electronic Storage" Contradicts the Plain Language of the Statute

"Electronic storage" is defined by statute to mean "(A) any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). In Theofel, the panel held that "e-mail messages were in electronic storage regardless of whether they had been previously delivered." Slip op. at 12346. The panel did not dispute that delivered e-mail did not fit "within the purview of subsection (A)," because delivered e-mail is not in "temporary, intermediate" storage. Slip op. at 12345. However, the panel incorrectly held that delivered e-mail fell within the scope of § 2510(17)(B) because messages remain stored on the ISP as a "backup" for the user. Slip op. at 12345.

The holding that e-mail that has been delivered remains in "electronic storage" conflicts with the plain language of the Stored Communications Act ("SCA"). As an initial matter, the panel treated the "backup" subsection of the

definition (§ 2510(17)(B)) as independent of the "temporary, intermediate" subsection (§ 2510(17)(A)). The panel noted that "[a]n obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again–if, for example, the message is accidentally erased from the user's own computer." Slip op. at 12345. The panel concluded that storage of delivered e-mail fell "literally" within the scope of "electronic storage." Id. However, § 2510(17)(B) refers to "any storage of such communication by an electronic communication service for purposes of backup protection of such communication" (emphasis added). The phrase "such communication" necessarily refers to the communications defined in subsection § 2510(17)(A): communications stored temporarily at an intermediate point in transmission. **Therefore § 2510(17)(B) can encompass only backup copies of communications which are themselves in temporary, intermediate storage incidental to transmission.**

In support of its contrary conclusion, the panel mistakenly asserted that a narrow interpretation of "electronic storage" would render § 2510(17)(B) superfluous. See Slip op. at 12346. This erroneous claim is based on the assumption that under the narrow interpretation of "electronic storage," backups must also be temporary. The panel asserted that "Fraser's [narrow] interpretation

[of electronic storage] renders subsection (B) essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as 'temporary, intermediate storage' within the meaning of subsection (A)." Slip op. at 12346 (emphasis added). However, under the plain language of § 2510(17)(B), the backup itself need not be temporary: what is essential is that the underlying communication be in temporary, intermediate storage. Thus, the panel grafted on an additional requirement (that backups be temporary) to the narrow meaning of § 2510(17)(B). Without this novel addition, § 2510(17)(B) is not superfluous under the narrow meaning of "electronic storage."

In this context, it is useful to consider what the term "backup" meant to the drafters of the SCA. In 1986, providers of electronic communication service commonly stored copies of files to protect against system failure. For example, the House Report on the SCA states that "[b]ack up protection preserves the integrity of the electronic communications system and to some extent preserves the property of users of such a system." H.R. Rep. No. 647, 99th Cong., 2d Sess., at 68 (1986). By including backup protections within the definition of "electronic storage," Congress ensured that backups would receive the same degree of protection as the underlying communications.

B. The Panel's Decision Threatens to Render Irrelevant Key Provisions of the Stored Communications Act

The structure of the SCA further demonstrates that "electronic storage" should not be given the expansive definition provided by Theofel. First, the panel's broad reading of "electronic storage" would render that statutorily defined term itself superfluous throughout the SCA. Second, the panel's broad interpretation of "electronic storage" also renders § 2702(a)(2) and § 2703(b) largely superfluous.

1. The Panel's Decision Renders Superfluous the Statutorily Defined Term "Electronic Storage"

Under Theofel, a backup falls within § 2510(17)(B) if it provides backup protection for either a user or a service provider. See Slip op. at 12345. Under this interpretation, any communication stored by an electronic communication service will be in "electronic storage." If a communication is in temporary, intermediate storage incident to transmission, it will fall under § 2510(17)(A). Any other copy of the communication stored by an electronic communication service will necessarily serve as a backup to either the user, the service, or both. Thus, any other copy will fall under § 2510(17)(B).

The defect in this reasoning is clear. If, as Theofel implies, any communication stored by an electronic communication service is in "electronic

storage," the term "electronic storage" becomes mere surplusage. In the SCA, the term "electronic storage" appears only in the following locations:

- § 2701(a) prohibits unauthorized access "to a wire or electronic communication while it is in electronic storage" in an electronic communication service (emphasis added).
- § 2702(a)(1) prohibits a provider of electronic communication service to the public from disclosing "the contents of a communication while in electronic storage" (emphasis added).
- § 2703(a) sets rules under which the government may compel a provider of electronic communication service to disclose either (1) "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less" (emphasis added) or (2) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days" (emphasis added).

In each of these sections, the underlined language is superfluous under the panel's decision.

2. The panel's broad interpretation of "electronic storage" renders § 2702(a)(2) and § 2703(b) largely superfluous, and this interpretation creates an unprecedented impediment to law enforcement

Far more importantly, the panel's decision effectively obliterates the SCA's essential distinction between two categories of communications: (1) electronic communications in "electronic storage" in an "electronic communication service" and (2) electronic communications stored by a "remote computing service."[1] As explained below, under Theofel, the former would swallow the latter.

i. Under the panel's broad interpretation of "electronic storage," § 2702(a)(2) and § 2703(b) serve no practical function in the Stored Communications Act

The dichotomy between communications in "electronic storage" and those not in "electronic storage" permeates the SCA. In adopting an overbroad reading of this defined term, the panel effectively eliminated this distinction.

For example, § 2703, which controls government access to stored communications, provides greater protection to communications in "electronic storage" than to other stored communications. Section 2703(a) provides that "[a] government entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that

---

[1] The term "remote computing service" is defined by 18 U.S.C. § 2711(2) as "provision to the public of computer storage or processing services by means of an electronic communications system."

is in electronic storage in an electronic communication system for one hundred and eighty days or less, only pursuant to a warrant . . ." (emphasis added). Thus, law enforcement can generally compel disclosures of e-mail "in electronic storage" only upon a showing of probable cause.[2]

In contrast, § 2703(b)(1)(B) allows law enforcement to compel a provider of "remote computing service" to disclose the contents of an electronic communication by means of a subpoena or a court order under 18 U.S.C. § 2703(d).[3] Thus, prosecutors can obtain access to files stored with a remote computing service using a standard lower than probable cause.[4]

This dichotomy between communications in "electronic storage" and other communications is mirrored in the SCA's rules relating to voluntary (not compulsory) disclosure of communications by network service providers. Under § 2702(a)(1), providers of electronic communication service are generally

---

[2] E-mail in "electronic storage" more than 180 days can be obtained by the government pursuant to a subpoena or 2703(d) order. See 18 U.S.C. § 2703(a) (stating that such communications can be compelled "by the means available under subsection (b) of this section").

[3] A 2703(d) order requires the government to offer "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

[4] Prosecutors retain the option of using a § 2703(a) search warrant to compel production of electronic communications stored by a remote computing service. See 18 U.S.C. § 2703(b)(1)(A).

prohibited from voluntarily disclosing user communications in "electronic storage." Providers of remote computing service – often the same entities – are prohibited by § 2702(a)(2) from voluntarily disclosing other user communications.

The communications governed by the precisely parallel non-"electronic storage" provisions, §§ 2702(a)(2) and 2703(b), are subject to additional (and identical) limitations. Each of these provisions applies explicitly to communications held by a service provider "solely for the purpose of providing storage or computer processing services to [the] subscriber or customer." § 2702(a)(2)(B); § 2703(b)(2)(B) (emphasis added). Plainly, communications within this category are **not** in "electronic storage," which is dealt with in parallel subsections (§§ 2702(a)(1) and 2703(a)), or these references to "providing storage ... to [the] subscriber" would be utterly superfluous. Yet the panel's decision declares that such convenience storage is a "backup" (and therefore within the meaning of "electronic storage"), abolishing a distinction written expressly into the Act. Such an interpretation renders largely superfluous § 2702(a)(2) and § 2703(b).

ii. The distinction between communications in "electronic storage" and other stored communications is critical to law enforcement

The distinction between electronic communications in "electronic storage" and subject to the requirements of § 2703(a) and other electronic communications subject to § 2703(b) is critical for law enforcement, because § 2703 places greater restrictions on government access to communications in electronic storage. As traditionally understood by Congress, other courts, and the Department of Justice, the term "electronic storage" is much more limited than its everyday meaning. Under this traditional interpretation, "electronic storage" refers only to temporary storage, made in the course of transmission, by a provider of electronic communications service, and to backups of such intermediate communications. See Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp.2d 623, 636 (E.D. Pa. 2001) (stating that "[t]he phrase 'for purposes of backup protection of such communication' in the statutory definition makes clear that messages that are in post-transmission storage, after transmission is complete, are not covered by part (B) of the definition of 'electronic storage'"); In re Doubleclick Inc. Privacy Litigation, 154 F. Supp.2d 497, 511-13 (S.D.N.Y. 2001) (emphasizing that "electronic storage" should have a narrow interpretation based on statutory

interpretation and legislative intent)[5]; Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 86-87 (2d ed. 2002), available at http:\\www.cybercrime.gov/s&smanual2002.pdf.

Under this narrow interpretation of "electronic storage," a copy of an e-mail is in "electronic storage" only if it is at an intermediate point in its transmission and has not yet been sent on to its final destination, the recipient of the e-mail. If an e-mail has been received by a recipient's ISP but has not yet been accessed by the recipient, it is in "electronic storage." Once the recipient retrieves the e-mail, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the e-mail on the ISP's system, the copy on the network is no longer in "electronic storage" because it is no longer in "temporary, intermediate storage . . . incidental to . . . electronic transmission." See Orin S. Kerr, A User's Guide to the Stored Communications Act–And A Legislator's Guide to Amending It, Geo. Wash. L. Rev. (forthcoming 2004), available at http:\\papers.ssrn.com/sol3/papers.cfm?abstract_id=421860, at 7-8 (draft).

---

[5] In interpreting the term "electronic storage" narrowly, the Doubleclick court also relied upon the canon of statutory interpretation which disfavors a broad reading of a criminal statute. See Doubleclick, 154 F. Supp.2d at 513. That rule is equally applicable to Theofel. Although Theofel is a civil suit under § 2707 of the SCA, civil liability under § 2707 for a violation of § 2701 is coextensive with criminal liability under § 2701. Because Theofel reads "electronic storage" expansively, it also reads criminal liability under § 2701 expansively, contrary to the canons of statutory interpretation. See Jones v. United States, 529 U.S. 848, 858 (2000).

Even under this traditional interpretation of "electronic storage," opened and retained e-mail stored with an ISP is not without protection under the SCA. However, its categorization under the SCA changes once a copy is delivered to its intended recipient, and it receives somewhat less privacy protection. Such e-mail retained on the provider's system is no longer an "electronic communication . . . in electronic storage;" instead, it becomes an electronic communication stored by a "remote computing service." See id.

Combining the structure of § 2703(a) and (b) with the traditional interpretation of the status of e-mail under the SCA yields the following framework for compelling disclosure of e-mail, which until now has been followed by federal prosecutors nationwide:

- Unopened e-mail stored on an ISP's servers constitutes electronic communications in electronic storage. Such e-mail can be obtained only using a warrant based on probable cause, unless it is more than 180 days old.
- Opened e-mail or copies of sent e-mail retained by users constitute files stored with a remote computing service. Such files can be obtained pursuant to § 2703(b)(1)(B) using a subpoena or 2703(d) order, or pursuant to § 2703(b)(1)(A) using

a warrant based on probable cause.

Theofel overturns this framework. Under Theofel, all copies of e-mail stored by a network services provider constitute electronic communications in electronic storage and hence are available to law enforcement only pursuant to a warrant based on probable cause, unless they are more than 180 days old. Substantial quantities of evidence previously available to state and federal prosecutors are no longer available under this heightened standard. Such evidence is often critical in a broad spectrum of cases, including cases involving network intrusion, fraud, child pornography, and illegal drugs. The significance of this change for law enforcement cannot be overstated.

In addition, because the Internet spans state borders, Theofel is likely to create conflicts for law enforcement nationwide. Network service providers who violate the SCA are subject to civil suit under § 2707. They may face civil suits in the Ninth Circuit for responding to government process under § 2703(b) from outside the Ninth Circuit. Such suits are particularly likely to be a problem for service providers located in the Ninth Circuit, like Hotmail and Yahoo!. Alternatively, network service providers outside the Ninth Circuit may fear lawsuits brought by customers within the Ninth Circuit. Network service providers may begin to resist subpoenas and 2703(d) orders under § 2703(b), even when that

process does not come from the Ninth Circuit. Thus, Theofel will likely prove disruptive for law enforcement nationwide.

II. THE PANEL'S INTERPRETATION OF "ELECTRONIC STORAGE" CONFLICTS WITH THE STORED COMMUNICATIONS ACT'S LEGISLATIVE HISTORY

The error in the panel's holding – that e-mail is in "electronic storage" regardless of whether it has been delivered – is further confirmed by the SCA's legislative history. As explained below, Congress intended a much narrower reading of "electronic storage." For that reason, the Petition for Rehearing should be granted.

In the course of considering the SCA's prohibitions on voluntary disclosure by network service providers of customer communications, the drafters of the SCA in 1986 explicitly considered what would happen when a recipient of e-mail kept a copy of the e-mail on his ISP after receipt:

> Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. The Committee intends that, in leaving the message in storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, and that such communication should continue to be covered by section 2702(a)(2).

H.R. Rep. No. 647, 99th Cong., 2nd Sess., at 65 (1986) (emphasis added). As explained above, § 2702(a)(2) prohibits disclosure of communications stored by a remote computing service, rather than communications in "electronic storage" in

an electronic communication service (which are covered by § 2702(a)(1)). The House Report in effect says the following: when a customer opens an e-mail message and leaves a copy on the ISP server, the copy is treated as a communication maintained by a remote computing service.

Subsequent legislative history confirms Congress's continued understanding that previously delivered e-mail maintained by an ISP is not in electronic storage. In 2000, Congress considered and rejected amending the definition of electronic storage to include "any storage of an electronic communication by an electronic communication service without regard to whether the communication has been accessed by the intended recipient." See H.R. Rep. No. 932, 106th Cong., 2nd Sess. at 7 (2000) (emphasis added). The drafters of this amendment understood that previously accessed e-mail did not fall within the scope of § 2510(17).

In addition, the House Report on the USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), demonstrated Congress's narrow understanding of the term "electronic storage." In the course of discussing an amendment to the SCA allowing for nationwide service of § 2703(a) warrants, the Report states that "2703(a) requires a search warrant to compel service providers to disclose unopened e-mails." H.R. Rep. No. 236(I), 107th Cong., 1st Sess. at 57 (2001) (emphasis added). Because warrants under § 2703(a) are required only for

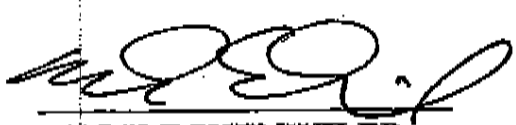
electronic communications in "electronic storage," this statement is further evidence that Congress did not intend opened e-mail to fall within the scope of "electronic storage." The panel has supplied the term "electronic storage" with a meaning rejected by Congress, thereby creating difficulties for law enforcement. Therefore, the Petition for Rehearing should be granted.

CONCLUSION

For the foregoing reasons, this Court should grant the Petition for Rehearing.

Respectfully submitted.

CHRISTOPHER A. WRAY
Assistant Attorney General

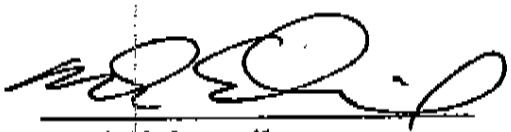


MARK ECKENWILER
Deputy Chief
Computer Crime and Intellectual
Property Section

NATHAN JUDISH
Attorney, Computer Crime and
Intellectual Property Section
Criminal Division
U.S. Department of Justice
Washington, D.C. 20530

CERTIFICATE OF COMPLIANCE

I certify that pursuant to Circuit Rules 35-4 and 40-1 the attached Brief for the United States as Amicus Curiae Supporting Defendant/Appellee's Petition for Rehearing and Suggestion for Rehearing En Banc is proportionately spaced, has a typeface of 14 points, and contains 4136 words as counted by the word processing system on which it was prepared.



Mark Eckenwiler

CERTIFICATE OF SERVICE

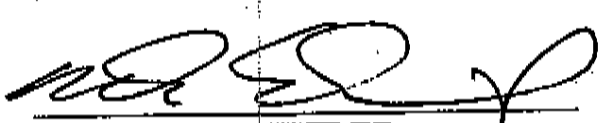
I HEREBY CERTIFY that two copies of the foregoing Brief for the United States as Amicus Curiae Supporting Defendant/Appellee's Petition for Rehearing and Suggestion for Rehearing En Banc were this day sent by regular mail to the following person(s):

Robert E White
Susan C. Rushakoff
Law Offices of Robert E. White
177 Post Street, Suite 890
San Francisco, CA 94108

James M. Wagstaffe
Pamela Urueta
Kerr & Wagstaffe LLP
100 Spear Street, Suite 1800
San Francisco, CA 94105

Richard Idell
Jennifer Marone
Idell, Berman & Seitel
530 Bush Street, Suite 601
San Francisco, CA 94105

Iryna A. Kwasny
Environmental Law Foundation
1736 Franklin Street, 9th Floor
Oakland, CA 94612



MARK ECKENWILER
Deputy Chief
U.S. Department of Justice
Criminal Division
Computer Crime and Intellectual
Property Section
1301 New York Avenue. NW
Suite 600
Washington, D.C. 20530
(202) 514-1026

Dated: SEPTEMBER 25, 2003