

---

Nos. 02-CV-72054-DT

---

UNITED STATES COURT OF APPEALS  
FOR THE SIXTH CIRCUIT

---

JEFFREY KLIMAS, individually and  
as a Class Representative,

Plaintiff-Appellant,

v.

COMCAST CABLE COMMUNICATIONS, INC.,

Defendant-Appellee,

---

Kevin Bankston  
Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, CA 94110  
(415) 436-9333 x 102  
(415) 436-9993 – facsimile

Attorneys for Amicus Curiae

---

**BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER  
FOUNDATION SUPPORTING REVERSAL OF THE DISTRICT  
COURT’S GRANTING OF DEFENDANT’S MOTION TO DISMISS**

**TABLE OF CONTENTS**

I. STATEMENT OF AMICUS CURIAE..... 1

II. INTRODUCTION..... 2

III. STATUTORY FRAMEWORK..... 4

IV. ARGUMENT ..... 5

    A. “Personally identifiable information” is information that is  
    reasonably capable of identifying a person. .... 5

    B. IP addresses are “personally identifiable information” because  
    they can easily be used to identify persons. .... 8

    C. The privacy interest in records of what a person communicates,  
    reads or views is especially great. .... 11

    D. The district court’s reasoning about IP addresses threatens to  
    negate statutory privacy protections. .... 13

V. CONCLUSION..... 14

**TABLE OF AUTHORITIES**

**Cases**

*Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539 (1963) ..... 12

*McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995) ..... 11

*NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958) ..... 12

*Roaden v. Kentucky*, 413 U.S. 496 (1973) ..... 12

*Shelton v. Tucker*, 364 U.S. 479 (1960)..... 12

*Stanford v. Texas*, 379 U.S. 476 (1965)..... 12

*Talley v. California*, 362 U.S. 60 (1960) ..... 12

**Statutes**

Cable Communications Policy Act of 1984, 47 U.S.C. § 551 .....passim

Children’s Online Privacy Protection Act, 15 U.S.C. § 6501(8) ..... 14

Electronic Communications Privacy Act, 18 U.S.C. § 2703(c)(2)(E)..... 10

Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320 ..... 6, 9

Privacy Act of 1974, 5 U.S.C. § 552(e)(7)..... 12

Telecommunications Act of 1996, 47 U.S.C. § 222(c)(3)..... 14

Video Privacy Protection Act, 18 U.S.C. § 2710(b)(1)..... 14

**Other Authorities**

45 C.F.R. Parts 160, 164 ..... 6

64 Fed.Reg. 59,918 (1999) ..... 7

Final Rule, 65 Fed.Reg. 82,462 (2002)..... 7

H.R. 69 §8(8)..... 8

H.R.Rep. No. 934, 98th Cong., 2d Sess. 29 (1984), reprinted in 1984  
U.S.Code Cong. & Admin.News (U.S.C.C.A.N.) 4655 ..... 5

S. Rep. 100-599, 100th Cong., 2d Sess. 7 (1988), reprinted at 1988  
U.S.C.C.A.N. 4342..... 14

**Books and Articles**

Computer Crime and Intellectual Prop. Div., U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* Sec. III(C)(1) (2002)..... 10

Craig Hunt, *TCP/IP Network Administration* 12 (O'Reilly 1998) ..... 8

Preston Gralla, *How the Internet Works* 155 (Que 1999)..... 2

*Webster's New World Dictionary* 696 (2<sup>nd</sup> college ed. 1986)..... 6

*Webster's Third New Int'l Dict.* 1123 (1986)..... 6

**DISCLOSURE OF CORPORATE AFFILIATIONS AND  
OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN  
LITIGATION**

Pursuant to FRAP 26.1, amicus Electronic Frontier Foundation ("EFF"), a 501(c)(3) non-profit corporation incorporated in the State of Massachusetts makes the following disclosure:

1. EFF is not a publicly held corporation or other publicly held entity.
2. EFF has no parent corporations.
3. No publicly held corporation or other publicly held entity owns 10% or more of EFF.
4. EFF is not a trade association.

April 6, 2004

---

Kevin Bankston  
Attorney  
Electronic Frontier Foundation

## I. STATEMENT OF AMICUS CURIAE

The Electronic Frontier Foundation ("EFF") is a non-profit, civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges industry and government to support free expression, privacy, and openness in the information society. Founded in 1990, EFF is based in San Francisco. EFF has members all over the United States and maintains one of the most-linked-to Web sites in the world. (<http://www.eff.org>)

EFF believes that privacy is a fundamental human right. While the vast web of electronic media that now connects us has great potential to empower individuals, it has also created new threats to personal privacy: when we use the Internet, we leave easily collected digital footprints of where we go - from online stores that reflect our buying preferences as consumers to websites that reflect our religious, political, cultural and other interests and beliefs as citizens.

EFF writes solely to address the meaning of the phrase "personally identifiable information." As we explain below, the very concept of identifiability must be understood in light of the ever-increasing accumulation of information about us in myriad computer databases. In this age of "data-mining," the concept of identifiability has serious implications beyond the instant case.

Because defendant Comcast has not consented to the filing of this amicus brief, EFF is moving this Court for leave to file.

## II. INTRODUCTION

For a few months, defendant Comcast collected information about its subscribers' on-line activities, such as the websites they visited and other information that they sent or received during their time on-line. R. 22 Complaint, ¶¶ 37, 43. This information was indexed by subscribers' Internet Protocol (IP) addresses<sup>1</sup> rather than their actual names. *Id.* at ¶¶38, 42, 43. In essence, instead of (hypothetically) recording that "John Smith" had visited a particular URL<sup>2</sup> like <http://www.amazon.com>, Comcast recorded that "111.222.255.4" had visited <http://www.amazon.com>. However, Comcast keeps records of which IP address is assigned to which subscriber at which time. *Id.* at ¶¶ 23, 40. Comcast therefore knows that our hypothetical John Smith corresponds to 111.222.255.4.

The immediate issue of concern to amicus in this case is whether IP addresses and information linked to IP addresses constitute "personally identifiable information" under the privacy provision of the Cable Communications Policy Act of 1984 (CCPA), 47 U.S.C. § 551. The more general question is whether information pertaining to a person is "personally

---

<sup>1</sup> For present purposes, an IP address is like a telephone number; it identifies the point from which an Internet user connects to the Internet. Just as one cannot use the telephone system without a telephone number assigned by your telephone company, you cannot use the Internet without an IP address (e.g., 111.222.255.4) assigned to you by your Internet service provider (ISP). The only exception is when you use someone else's Internet connection, such as at work, a public library, a university, or private home network.

<sup>2</sup> URL stands for "Uniform Resource Locator"; URLs are used to describe the location of web pages on the Internet. Preston Gralla, *How the Internet Works* 155 (Que 1999).

identifiable” when it lacks identifiers such as the person’s name, address or telephone number, but the person can readily be identified with other information – such as Comcast’s database that maps subscribers to their IP addresses.

Amicus EFF contends that the district court erred in concluding that subscribers’ IP addresses and information linked to subscribers’ IP addresses are not “personally identifiable information” under the CCPA. Amicus further contends that the district court’s erroneous holding has dangerous implications for privacy beyond the instant case.

The district court’s conclusion that IP addresses are not “personally identifiable information” was apparently based on its assumption that the IP addresses at issue in this case are “dynamic,” not “static,” and the fact that dynamic IP addresses constantly change. Op. at 7. On these premises, the district court found that “unless an IP address is correlated to some other information . . . it does not identify any single subscriber by itself” and cannot be “personally identifiable information.” Op. at 7. Accordingly, the court also determined that Comcast’s collection of IP-URL linkages also was not “personally identifiable information.” Op. at 8.

The flaw in this logic is obvious. Most personally identifiable information does not identify a specific person “by itself”; it must be correlated to some other information to be useful. For example, without the equivalent of a reverse telephone directory, a person’s telephone number is just a telephone number. Even a name does not necessarily identify a

specific person without more information; many men are named David Nelson, for example. Amicus is concerned that if the district court's approach to "personally identifiable information" is upheld, other laws that use the concept of "identifiability" will also be weakened.

Finally, amicus notes that the information at issue in this case is especially personal because it includes information about what subscribers communicated, viewed or read on-line. U.S. law has long recognized that information about the exercise of First Amendment rights is especially sensitive from a privacy standpoint. Further considering that identity theft has made the privacy of personal information a significant social and political issue, this Court should reject the district court's flawed logic and erroneous conclusion.

### **III. STATUTORY FRAMEWORK**

The CCPA generally prohibits cable operators from collecting or disseminating their subscribers' "personally identifiable information" without subscriber consent. 47 U.S.C. § 551(b)(1) ("a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.").

The CCPA was enacted out of Congressional concern about the "enormous capacity" of "[c]able systems, particularly those with a 'two-way' capability . . . to collect and store personally identifiable information about each cable subscriber." H.R.Rep. No. 934, 98th Cong., 2d Sess. 29 (1984),

reprinted in 1984 U.S.Code Cong. & Admin.News (U.S.C.C.A.N.) 4655, 4666. "Subscriber records from interactive systems can reveal details about bank transactions, shopping habits, political contributions, viewing habits and other significant personal decisions." Id.

Accordingly, cable subscribers have the right to access and correct errors in "all personally identifiable information regarding that subscriber which is collected and maintained by a cable operator." 47 U.S.C. § 551(d). Moreover, the cable operator "shall destroy personally identifiable information" once it is no longer needed for the purpose for which it was collected and there are no pending requests for that personally identifiable information. 47 U.S.C. § 551(e).

The CCPA does not define "personally identifiable information," but it does exclude "any record of aggregate data which does not identify particular persons." 47 U.S.C. § 551(a)(2)(A). The CCPA's legislative history further notes that "personally identifiable information" "would include specific information about the subscriber, or a list of names and addresses on which the subscriber is included, but does not include aggregate information about subscribers which does not identify particular persons." 1984 U.S.C.C.A.N. 4655, 4716.

#### IV. ARGUMENT

A. **"Personally identifiable information" is information that is reasonably capable of identifying a person.**

The district court confused the term "personally identifying

information” with “personally identifiable information.” Standard dictionary definitions demonstrate that “identifying” is not equivalent to “identifiable.” “Identifying” is the inflected form of “identify,” which means “to recognize as being or show to be the very person or thing known, described or claimed; fix the identity of.” *Webster’s New World Dictionary* 696 (2<sup>nd</sup> college ed. 1986). “Identifiable,” on the other hand, means “subject to identification; capable of being identified.” *Webster’s Third New Int’l Dict.* 1123 (1986).

The most sophisticated treatment of personal “identifiability” has been developed under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which seeks to protect the privacy of “individually identifiable health information.” 42 U.S.C. § 1320d, -1 to -8 (Supp. V 1999). Pursuant to HIPAA, the Department of Health and Human Services (DHHS) promulgated “Standards for Privacy of Individually Identifiable Health Information” (HIPAA Privacy Standards) that cover “all individually identifiable health information in any form . . . that is held or transmitted by a covered entity.” 65 Fed. Reg. 82,462, 82,488 (Dec. 28, 2000) (codified at 45 C.F.R. Parts 160, 164).

Because HIPAA only protects “individually identifiable health information,” it was necessary for DHHS to articulate when health information is not “individually identifiable.” DHHS ultimately determined that “[h]ealth information that does not identify an individual and with respect to which there is no reasonable basis to believe that it can be used to identify the individual is not individually identifiable health information.”

45 C.F.R. § 164.514(a).

DHHS observed that “[i]t is not always obvious when information identifies the subject.” 64 Fed.Reg. 59,918, 59,935 (1999) (Proposed Rules for HIPAA Privacy Standards). DHHS was influenced by statistical research showing that seemingly de-identified data could be easily re-identified. “A 1997 MIT study showed that, because of the public availability of the Cambridge, Massachusetts voting list, 97 percent of the individuals whose data appeared in a data base which contained only their nine-digit zip code and birth date could be identified with certainty.” Id. at 59,935 (citation omitted).

Accordingly, in promulgating the final rules, DHHS rejected commenters’ suggestions that removing only “direct” identifiers like name, address and ID numbers would render health information not “individually identifiable” because “the resulting information would often remain identifiable.” Final Rule, 65 Fed.Reg. 82,462, 82,708 (2002).

Similarly, Congress recognized in the proposed Online Privacy Protection Act of 2003 that “personal information” in the Internet context means

“information collected online from an individual that identifies the individual, including (A) first and last name; (B) home and other physical address; (C) e-mail address; (D) social security number;(E) telephone number; (F) any other identifier that the Commission determines identifies an individual; or (G) information *that is maintained with, or can be searched or*

*retrieved by means of, data described in subparagraphs (A) through (F).*<sup>3</sup>

Here, Congress recognizes that the connections between pieces of information can determine the capability of information to identify an individual.

In short, “personally identifiable information” should not be limited to information that contains a subscriber’s name, address or telephone number; it must include information that is reasonably capable of identifying the subscriber in combination with other information.

**B. IP addresses are “personally identifiable information” because they can easily be used to identify persons.**

Although an IP address<sup>4</sup> is a series of numbers assigned to a computer on the Internet, it can still potentially identify a person and is therefore “identifiable.” Blocks of IP addresses are delegated to Internet service providers (ISPs). As part of providing Internet service, the ISP then delegates one or more IP addresses to its subscribers, and can maintain

---

<sup>3</sup> H.R. 69 §8(8) (emphasis added). Full Title: To require the Federal Trade Commission to prescribe regulations to protect the privacy of personal information collected from and about individuals who are not covered by the Children's Online Privacy Protection Act of 1998 on the Internet, to provide greater individual control over the collection and use of that information, and for other purposes. Sponsored by Rep. Frelinghuysen, [NJ-11]; (introduced 1/7/2003).

<sup>4</sup> The Internet Protocol (IP) is the “building block of the Internet” and is the means by which data traverses the Internet. Craig Hunt, *TCP/IP Network Administration* 12 (O’Reilly 1998). In order to properly deliver data, IP addresses are used throughout the Internet to uniquely identify every host (e.g., computer) on the network. *Id.* at 23. Roughly analogous to telephone numbers in the telephone systems, IP addresses identify the source and destination for data traveling along the Internet.

records of which IP addresses are assigned to each subscriber. By proxy, these records turn IP addresses into information that can uniquely identify ISP subscribers. If the subscriber is a small enough group (as with a family at home), an IP address is as useful in identifying a person as a home telephone number.

Although the IP address does not “by itself” identify an individual subscriber, it is still effectively personally identifiable information when coupled with ISP records that link IP addresses to subscribers. Because Comcast keeps records of which IP addresses belong to which subscriber at any given time, R. 22 Complaint, ¶¶ 37, 43, it can easily identify the subscriber that used a particular IP address at a particular time, or identify the IP address that a particular subscriber used at a particular time. Thus, in this case the IP addresses assigned to subscribers are clearly “personally identifiable information.”

The HIPAA Privacy Standards are consistent with this conclusion. IP addresses are among the individually identifying facts that must be removed from health information before it can be deemed “de-identified.” 45 C.F.R. § 164.514(b)(2)(i).<sup>5</sup> Such facts include name, geographic location information, dates (e.g., birth and death dates), telephone numbers, fax numbers, e-mail addresses, social security numbers, medical record

---

<sup>5</sup> Alternatively, the entity covered by HIPAA may hire an expert to alter the data so that there is only a tiny risk that the information could be used to identify a patient. 45 C.F.R. § 164.514(b)(1).

numbers, Web Universal Resource Locators (URLs), IP address numbers, biometric identifiers like finger and voice prints, and full-face photographs. Ibid.

Law enforcement also uses IP addresses to identify people. Under the Electronic Communications Privacy Act (ECPA), “any temporarily assigned network address” is a type of “subscriber number or identity.” 18 U.S.C. § 2703(c)(2)(E). ECPA more generally defines “basic subscriber information” to also include name, address, telephone records, records of session times and durations, and length of service. *Id.* at § 2703(c)(2)(A)-(D). The Justice Department notes that

In general, the items in this list relate to the identity of a subscriber, his relationship with his service provider, and his basic session connection records.... In the Internet context, these records include the IP address assigned by an Internet service provider to a customer for a particular session. They also include other information relating to account access, such as the originating telephone number for dial-up Internet access or the IP address of a user accessing an account over the Internet.

Computer Crime and Intellectual Prop. Div., U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* Sec. III(C)(1) (2002), available at <http://www.cybercrime.gov/s&smanual2002.htm>. As a result, there can be no doubt that IP addresses are “personally identifiable information.”

The district court found that neither dynamic IP addresses nor information linked to dynamic IP addresses, such as URLs, could be “personally identifiable information.” *Op.* at 8. Apparently important to the

district court's finding was the fact that dynamic IP addresses constantly change, so that they are more like hotel rooms than relatively unchanging residence addresses. The district court did not make a finding about static IP addresses, which it presumably would have analogized to home addresses.

This distinction is untenable. There is nothing inherently identifying in an IP address, whether or not it changes or remains the same. This Court would be hard-pressed to identify anyone from a list of either static or dynamic IP addresses without additional information. Conversely, Comcast – or any other ISP – can easily identify its subscribers from a list of IP addresses, whether static or dynamic, because it maintains a database that maps its subscribers to the IP addresses it assigns to them. The only difference between static and dynamic IP addresses is that the ISP constantly updates the mapping between the subscribers and dynamic IP addresses. The real issue is not whether IP addresses change, but whether the ISP can link the IP address to the subscriber.

**C. The privacy interest in records of what a person communicates, reads or views is especially great.**

The district court's errors here are especially serious because reading and viewing records have long been considered sensitive, not only in terms of privacy, but in terms of freedom of expression. First Amendment law has long protected privacy in order to protect freedom of speech and association. See *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 355 (1995) (striking down law forbidding distribution of anonymous election-related literature);

*Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 558 (1963) (rejecting attempt of Florida legislative committee to require NAACP to produce membership records); *Shelton v. Tucker*, 364 U.S. 479, 490 (1960) (striking down state statute requiring that teachers list all of their association memberships in the previous five years); *Talley v. California*, 362 U.S. 60, 64 (1960) (declaring unconstitutional blanket prohibition on anonymous handbill distribution); *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460 (1958) (holding that requiring NAACP to produce membership records would chill association).

Similarly, Fourth Amendment law has long recognized that when expressional materials are the subject of search or seizure, its requirements must be observed with “scrupulous exactitude.” *Stanford v. Texas*, 379 U.S. 476, 485 (1965); see *Roaden v. Kentucky*, 413 U.S. 496, 501-502 (1973) (distinguishing seizures of books or movies from other things). Also, the Privacy Act of 1974 gives special protection to information concerning the exercise of First Amendment rights. 5 U.S.C. § 552(e)(7).

Clearly, Congress’s concern that “[s]ubscriber records from interactive systems can reveal details about bank transactions, shopping habits, political contributions, viewing habits and other significant personal decisions” requires this Court to read the CCPA’s privacy provisions broadly in order to effectuate Congressional intent.

**D. The district court’s reasoning about IP addresses threatens to negate statutory privacy protections.**

Finally, the district court’s approach to “identifiability” poses a broad threat to personal privacy that goes far beyond the present case, and may negate privacy protections offered by not only the CCPA but a number of other statutes.

Plaintiff alleged that Comcast had “the power to connect and correlate those online activities with the identity of each subscriber.” SAC ¶ 40. But the district court found that “[t]he fact that Comcast may have had the power to make such a correlation does not render the information PII.” Op. at 8.

In the CCPA context, however, this means that any cable operator could collect and store information about what its subscribers read or view on-line with impunity so long as such reading or viewing information was linked to its subscribers’ dynamic IP addresses, even when it always keeps track of which subscriber is using any given IP address. Moreover, both the subscriber’s statutory rights of access and correction and the cable operator’s duty to destroy information no longer needed for the purpose for which it was collected would be meaningless, because these rights only apply to “personally identifiable information.” 47 U.S.C. §§ 551(d), (e). Such a result would eviscerate the CCPA’s privacy provisions.

More generally, the district court in effect endorsed a superficial technique of breaking collections of personally identifiable information into pieces. For example, a list of names and book purchases could be transformed into non-personally identifiable information by turning it into

two lists: one that links a number to the name, and another that links the book purchases to the numbers. But no matter how many pieces are created by breaking up the original list, it will be trivial in this age of computers to put the pieces back together and identify who bought what book.

Other statutes also use the concept of “personal identifiability.” The Video Privacy Protection Act generally prohibits video stores from knowingly disclosing “personally identifiable information” concerning its customers, 18 U.S.C. § 2710(b)(1),<sup>6</sup> and its legislative history indicates that “personally identifiable information” is “information that links the customer or patron to particular materials or services.” S. Rep. 100-599, 100th Cong., 2d Sess. 7 (1988), reprinted at 1988 U.S.C.C.A.N. 4342, 4342-7. See also Telecommunications Act of 1996, 47 U.S.C. § 222(c)(3); Children’s Online Privacy Protection Act, 15 U.S.C. § 6501(8). The district court’s flawed logic may endanger these privacy-protecting statutes as well.

## V. CONCLUSION

The District Court misinterpreted “personally identifiable information” as “personally identifying information.” In so doing, the court set a precedent that threatens individual privacy on the Internet and potentially eviscerates the privacy protections in current statutes. For the foregoing reasons, the decision of the District Court should be reversed.

---

<sup>6</sup> The VPPA contains exceptions to this prohibition. 18 U.S.C. § 2710(b)(2).

DATED: April 6, 2004

By \_\_\_\_\_  
Kevin Bankston  
ELECTRONIC FRONTIER  
FOUNDATION  
454 Shotwell Street  
San Francisco, CA 94110  
Telephone: (415) 436-9333 x 102  
Facsimile: (415) 436-9993

Attorneys for Amicus Curiae  
ELECTRONIC FRONTIER  
FOUNDATION

**CERTIFICATE OF COMPLIANCE**

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 3,311 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2000 version 9 in Times New Roman, 14-point font.

DATED: April 6, 2004

By \_\_\_\_\_  
Kevin Bankston  
ELECTRONIC FRONTIER  
FOUNDATION  
454 Shotwell Street  
San Francisco, CA 94110  
Telephone: (415) 436-9333 x 102  
Facsimile: (415) 436-9993

Attorneys for Amicus Curiae  
ELECTRONIC FRONTIER  
FOUNDATION

**CERTIFICATE OF SERVICE**

I certify that, on this 6th day of April, 2004, two (2) true and correct copies of Brief of Amicus Curiae Electronic Frontier Foundation Supporting Reversal of the District Court's Granting of Defendant's Motion to Dismiss were served via Federal Express, Overnight Delivery, upon the following:

Seth Lesser  
Locks Law Firm, PLLC  
110 East 55th Street  
New York, NY 10022

Thomas J. Tallerico  
John A. Behrendt  
Bodman, Longley  
201 W. Big Beaver Road, Suite 500  
Troy, MI 48084

Steven E. Goren  
Goren, Goren & Harris, P.C.  
30400 Telegraph Road, Suite 470  
Bingham Farms, MI 48025

Jaime Bianchi  
White & Case  
200 S. Biscayne Boulevard  
Suite 4900  
Miami, FL 33131-2352

---

Kevin Bankston  
Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, CA 94110  
(415) 436-9333 x 108

Attorney for Electronic Frontier Foundation

April 6, 2004