

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JOHN DOE and AMERICAN CIVIL
LIBERTIES UNION,

Plaintiffs,

v.

JOHN ASHCROFT, in his official capacity as
Attorney General of the United States;
ROBERT MUELLER, in his official
capacity as Director of the Federal Bureau of
Investigation; and MARION E. BOWMAN,
in his official capacity as Senior Counsel to
the Federal Bureau of Investigation,

Defendants.

Case No. 04 Civ 2614(VM)

**BRIEF OF ELECTRONIC FRONTIER FOUNDATION, ET AL., AS *AMICUS CURIAE*
IN SUPPORT OF PLAINTIFFS JOHN DOE AND AMERICAN CIVIL LIBERTIES
UNION**

TABLE OF CONTENTS

I. PRELIMINARY STATEMENT	1
II. THE CHALLENGED STATUTE	1
III. INTERESTS OF AMICI.....	2
IV. ARGUMENT.....	4
A. NSL authority under Section 2709 reaches a broad range of sensitive records in the possession of a broad range of entities.	4
1. A broad range of Internet services providers is subject to Section 2709.....	4
2. Section 2709 reaches a broad range of sensitive records regarding expressive activity on the Internet.....	6
B. The First and Fourth Amendments protect the privacy of Internet users’ expressive activities.	8
C. Section 2709 unconstitutionally authorizes the FBI to demand a broad array of sensitive records protected by the First and Fourth Amendments.....	11
CONCLUSION.....	17

TABLE OF AUTHORITIES

Cases

<i>Andersen Consulting LLP v. UOP</i> , 991 F.Supp. 1041 (N.D. Ill. 1998).....	5
<i>Camara v. Municipal Court</i> , 387 U.S. 523 (1967)	11
<i>FTC v. Netscape Communications Corp.</i> , 196 F.R.D. 559 (N.D. Cal. 2000).....	5
<i>Gibson v. Fla. Legislative Investigation Comm.</i> , 372 U.S. 539 (1963)	9
<i>In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)</i> , 157 F.Supp.2d 286 (S.D.N.Y. 2001).....	5
<i>In re Doubleclick Inc. Privacy Litig.</i> , 154 F.Supp.2d 497 (S.D.N.Y. 2001)	5
<i>Konop v. Hawaiian Airlines, Inc.</i> , 302 F.3d 868 (9th Cir. 2002)	6
<i>Lamont v. Postmaster General</i> , 381 U.S. 301 (1965).....	9
<i>Martin v. City of Struthers</i> , 319 U.S. 141 (1943)	9
<i>McIntyre v. Ohio Elections Comm’n</i> , 514 U.S. 334 (1995).....	8, 9
<i>NAACP v. Alabama</i> , 357 U.S. 449 (1958).....	9
<i>Reno v. ACLU</i> , 521 U.S. 844 (1997).....	1, 10
<i>Roaden v. Kentucky</i> , 413 U.S. 496 (1973)	10
<i>Sheldon v. Tucker</i> , 364 U.S. 479 (1960).....	9
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979)	11, 12, 16
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965)	10
<i>Stanley v. Georgia</i> , 394 U.S. 557 (1969)	9
<i>Talley v. California</i> , 362 U.S. 60 (1960)	8
<i>United States v. Mullins</i> , 992 F.2d 1472 (9th Cir. 1993)	5
<i>United States v. New York Tel. Co.</i> , 434 U.S. 159 (1977)	12
<i>United States v. U.S. District Court</i> , 407 U.S. 297 (1972)	2, 11
<i>Watchtower Bible & Tract Soc’y of New York, Inc. v. Village of Stratton</i> , 536 U.S. 150 (2002).....	8
<i>Wolf v. Colorado</i> , 338 U.S. 25 (1949)	11

Statutes

18 U.S.C. § 2510, Electronic Communications Privacy Act, Pub. L. 99-508, Title II, 201[a],
100 Stat. 1867 (Oct.21, 1986)..... 1, 4, 6

18 U.S.C. § 2703(e) 7

USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) 2

Law Review Articles and Treatises

Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S.
CAL. L. REV. 1083 (2002)..... 12

Preston Galla, *How the Internet Works* (MacMillan Computer Publishing 1999) 4

U.S. Internet Service Provider Association, *Electronic Evidence Compliance – A Guide for
Internet Service Providers*. 18 BERKELEY TECH. L.J. 945 (2003) 6

The undersigned civil liberties and Internet services organizations the Electronic Frontier Foundation, the Center for Constitutional Rights, the Center for Democracy and Technology, the Electronic Privacy Information Center, the Online Policy Group, the Salon Media Group, Inc. and the U.S. Internet Industry Association respectfully submit this brief *amicus curiae* in support of plaintiffs' motion for summary judgment.

I. PRELIMINARY STATEMENT

Plaintiffs challenge the constitutionality of 18 U.S.C. § 2709, which authorizes the FBI to compel the production of subscriber and communications records in the possession of a broad range of Internet-related communications service providers, potentially covering billions of records from tens of thousands of entities. These demands, known as National Security Letters (NSLs), are issued without judicial oversight of any kind, yet allow the FBI to obtain a vast amount of constitutionally protected information. The statute is unconstitutionally overbroad because, on its face, it can be used to reach much protected speech yet is not narrowly tailored to serve a compelling government interest. Moreover, the vague language and broad sweep of the statute means that the FBI's use of NSLs is not cabined by any intelligible standard. The Internet is a new and powerful medium of expression that hosts millions of dialogues covering a range of topics "as diverse as human thought." *Reno v. ACLU*, 521 U.S. 844, 852 (1997). Countless of these dialogues occur anonymously or pseudonymously, whether through e-mail, message boards, or World Wide Web sites. Section 2709 facially violates the Constitution by allowing the FBI to obtain, without adequate procedural or substantive safeguards, First Amendment-protected records that identify previously anonymous Internet speakers, readers, and associations, as well as records that contain communications content protected by the Fourth Amendment. *Amici*, representing the interests of a broad range of Internet users and service providers, therefore submit this brief in support of plaintiffs' motion for summary judgment.

II. THE CHALLENGED STATUTE

Section 2709 of the Electronic Communications Privacy Act (ECPA), *see* Pub. L. 99-508, Title II, 201[a], 100 Stat. 1867 (Oct. 21, 1986) (codified as 18 U.S.C. § 2510, *et seq.*), provides

that:

A wire or electronic communications service provider [ECSP] shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation,

where the FBI director or his designee makes the required certification that the records sought “are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities....” 18 U.S.C. § 2709, as amended by the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001).

III. INTERESTS OF AMICI

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 and privacy 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>>.

The Center for Constitutional Rights (“CCR”) is a non-profit legal and educational organization that is dedicated to advancing and protecting the rights guaranteed by the United States Constitution and the Universal Declaration of Human Rights. Founded in 1966 during the civil rights movement, CCR has a long history of protecting individuals deemed by the government to pose a threat to national security from improper government surveillance. *See, e.g., United States v. United States District Court*, 407 U.S. 297 (1972); *Kinoy v. Mitchell*, 67 F.R.D. 1 (S.D.N.Y. 1975). Following the September 11, 2001 terrorist attacks on the United States, CCR has challenged a number of government measures taken in the name of national security that threaten our civil liberties. Among the suits it is litigating are: *Rasul v. Bush*, 124 S. Ct. 534 (2003); *Humanitarian Law Project v. Ashcroft*, 352 F.3d 382 (9th Cir. 2003); *Humanitarian Law Project v. Ashcroft*, No. CV 03-6107 ABC, 2004 U.S. Dist. LEXIS 926 (C.D. Cal. Jan. 23, 2004); and *Turkmen v. Ashcroft*, No. 02 CV 2307 (JG) (E.D.N.Y.).

The Center for Democracy and Technology (“CDT”), <<http://www.cdt.org>>, is a non-

profit public interest organization in Washington, D.C., dedicated to promoting civil liberties in this age of digital technologies, including advocating strong privacy protections for personal information and strong First Amendment protections for the Internet.

The Electronic Privacy Information Center ("EPIC") is a not-for-profit public interest research organization located in Washington, DC. EPIC's activities include the review of federal law enforcement activities and policies to determine their possible impacts on civil liberties and privacy interests. Among its other activities, EPIC publishes books, reports and a bi-weekly electronic newsletter. EPIC also maintains a heavily-visited site on the World Wide Web, <<http://www.epic.org>>, containing extensive information on emerging privacy issues.

The Online Policy Group ("OPG"), <<http://www.onlinepolicy.org>>, is a non-profit organization dedicated to online policy research, outreach, and action on issues such as access, privacy, the digital divide, and digital defamation. The organization fulfills its motto of "One Internet With Equal Access for All" through programs such as donation-based e-mail, e-mail newsletter hosting, Web site hosting, Internet domain registrations and colocation services, technical consulting, educational training, and refurbished computer donations. The California Community Colocation Project (CCCP) and QueerNet are OPG projects. OPG focuses on Internet participants' civil liberties and human rights, like access, privacy, and safety, and serves schools, libraries, the disabled, the elderly, youth, women, and sexual, gender, and ethnic minorities.

Salon Media Group's division the WELL, <<http://www.well.com>>, is a pioneering online gathering place that in its 19-year history has helped define the rights and responsibilities of participants in online communities. The WELL offers subscribers from around the world a members-only online discussion service providing award-winning forums, e-mail, Web publishing and intelligent conversation. The WELL spun off its ISP division in 1996 in order to focus on our core service of hundreds of featured discussion areas. The WELL is committed to providing individuals, groups and businesses with rich environments for exchange and expression, and with powerful tools and services to build and enhance public and private

communities.

The U.S. Internet Industry Association (“USIIA”) is a trade association with more than 200 members in Internet commerce, content, and connectivity. Its mission includes advocating deployment of broadband and advanced services, and supporting the growth and viability of the Internet industry.

IV. ARGUMENT

A. NSL authority under Section 2709 reaches a broad range of sensitive records in the possession of a broad range of entities.

1. A broad range of Internet services providers is subject to Section 2709.

“Electronic communications service” is broadly defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). An electronic communication is “any transfer of signs, signals, writing, images, sound, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce....” 18 U.S.C. § 2510(12).

Applying these definitions to the Internet¹, “ISPs such as America Online, Juno and

¹ A brief discussion of the Internet’s basic workings may be of aid to the Court (for an introductory volume on the subject suitable for a lay audience, see Preston Galla, *How the Internet Works* (MacMillan Computer Publishing 1999)):

The Internet is a global network of many individual computer networks, all speaking the same networking protocol, the **Internet Protocol (IP)**. Every computer connected to the Internet has an **IP address**, a unique numeric identifier that can be “static”, i.e. unchanging, or may be “dynamically” assigned by your ISP, such that your computer’s address changes with each new Internet session.

More sophisticated networking protocols may be “layered” on top of the IP protocol, enabling different types of Internet communications. For instance, **World Wide Web (Web)** communications are transmitted via the Hypertext Transfer Protocol (**HTTP**) and **e-mails** via the Simple Mail Transport Protocol (**SMTP**).

Additional protocols use their own types of addresses. For example, to download a **Web page**, you need its **Web address**, known as a Uniform Resource Locator (URL) (e.g., <http://www.eff.org>. To exchange e-mails, both the sender and recipient need **e-mail addresses** (e.g., user@isp.com). Computers that offer files for download over the Internet are called **servers** or **hosts**. For example, a computer that offers Web pages for download is called an HTTP server or Web host. Any computer may be server, client, or both, depending on the communication. The amount of data in an Internet communication is measured in **bytes**.

UUNet, as well as, perhaps, the telecommunications companies whose cables and phone lines carry the traffic" are ECSPs. *In re Doubleclick Inc. Privacy Litig.*, 154 F.Supp.2d 497, 511 n. 20 (S.D.N.Y. 2001). ECSPs also include providers of e-mail service that are not ISPs, e.g. Microsoft's free Web-based e-mail service Hotmail, <<http://www.hotmail.com>>, see *In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 157 F.Supp.2d 286, 289 (S.D.N.Y. 2001), Netscape's similar service via <<http://www.netscape.net>>, see *FTC v. Netscape Communications Corp.*, 196 F.R.D. 559, 560 (N.D. Cal. 2000), and the donation-based e-mail service *amicus* OPG offers to activist and progressive organizations,, <<http://www.onlinepolicy.org/services.shtml>>.

Similarly, services offering the capability to create e-mail "listservs" or mailing lists—essentially subscription e-mail newsletters—are likely to be considered ECSPs by the FBI. Examples again include OPG, which hosts 979 newsletters serving 111,187 subscribers, as well as the Yahoo! Groups service, <<http://groups.yahoo.com>>, which enables users to administer newsletters ranging over thousand of topics.

The "electronic communications service" definition is not limited to services provided to the general public. Hence any corporate office, school or library that offers its employees, students or members the means to access the Internet or otherwise communicate via an electronic network is an ECSP. See, e.g., *United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993) (airline that provides travel agents with computerized travel reservation system accessed through separate computer terminals can be an ECSP); *Andersen Consulting LLP v. UOP*, 991 F.Supp. 1041, 1042 (N.D. Ill. 1998) (Andersen, which has internal e-mail system, is an ECSP).

Although it has not been definitively litigated, it is also possible that providers hosting message boards or Web sites that allow visitors to post or send messages are ECSPs. See, e.g., *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 870 (9th Cir. 2002), cert. denied, 537 U.S. 1193

Communications to and from an Internet-connected computer occur through 65,536 different computer software **ports**. Many networking protocols have been assigned to particular **port numbers** by the Internet Engineering Task Force. For example, HTTP (Web) is assigned to port 80 and SMPT (e-mail) is assigned to port 25.

(U.S. Feb 24, 2003) (NO. 02-969) (court adopted parties' assumption that host of Web-based message board was ECSP). Such services would include amicus Salon Media Group's discussion forum the WELL, and amicus EFF's Action Alert service, <<http://action.eff.org>>, which allows visitors to the EFF Web site to send e-mails to their government representatives regarding online civil liberties issues.

Given the absence of judicial guidance in the matter, the FBI is likely to read the statute broadly, potentially reaching even individuals who host e-mail accounts or Web sites for friends and family. Even individuals who merely run a home wireless network that can be used to access the Internet by passersby outside the household may be treated by the FBI as an ECSP. What is clear is that rather than covering only traditional ISPs, the definition of electronic communications service likely encompasses services provided by tens if not hundreds of thousands of individuals and corporations, and that number will only grow as networking technology becomes cheaper, more powerful and more user-friendly.

2. Section 2709 reaches a broad range of sensitive records regarding expressive activity on the Internet.

Section 2709 is an “awkward” ECPA provision for ECSPs because in stating what records the FBI may demand, i.e. “subscriber information and toll billing records information, or electronic communication transactional records,” 18 U.S.C. § 2709, the statute uses terms that are not defined and do not appear elsewhere in ECPA. U.S. Internet Service Provider Association, *Electronic Evidence Compliance – A Guide for Internet Service Providers*. 18 BERKELEY TECH. L.J. 945, 974 (2003). Nor has any court considered the scope of these undefined terms, such as “electronic communication transactional records.”

Furthermore, insofar as the types of records obtainable with an NSL are in doubt, entities served with NSLs are in a poor position to act as a check on the FBI's behavior. Each NSL is accompanied by a gag order prohibiting the ECSP from ever revealing the demand was made, *see* 18 U.S.C. § 2709(d). As a result, each ECSP—alone, in secret, without being able to consult with other ECSPs and without the benefit of adequate legislative or judicial guidance—is left to

decide for itself whether the records demanded are properly within the reach of Section 2709. Nor can public opinion serve as a check against overbroad demands under Section 2709 since the public can never be told of these demands.

Accountability is further diminished by ECSPs' statutory shield from liability for complying with an NSL, *see* 18 U.S.C. § 2703(e), which gives the ECSPs themselves little incentive to litigate and thus gives courts little opportunity to review concerns over what records are covered by Section 2709. A plain reading of Section 2709 would at least include the following (*see generally* the Garfinkel Declaration in support of Plaintiff's Motion for Summary Judgment for greater technical detail and discussion of additional records):

- Subscriber **account information** such as (1) name, (2) address, (3) length of service and types of service subscribed to, and (4) the means and source of payment for the service, including any credit card or bank numbers.
- The subscriber's **e-mail address(es)** and those of each of the subscriber's correspondents.
- **E-mail "headers"** that contain addressing and routing information generated by the e-mail client and mailservers, including the e-mail address of the sender and recipient(s), as well as information about when each email was sent or received and what computers it passed through while traveling over the Internet.
- The **Web address** of every Web page or site accessed.
- The **IP address** assigned to the subscriber by the ECSP, and the IP addresses of other Internet-connected computers that the subscriber sent to or received from.
- The **port number** used, indicating the type of networking protocol used (e.g., HTTP, SMTP) and hence the type of communication (e.g., Web page, e-mail).
- **Web server logs** showing the source (i.e., IP address) of requests to view a particular Web page.
- **Connection logs** showing when the subscriber connected to and disconnected from the Internet.

- Time stamps showing the date and time when each communication was sent or received.
- The size in bytes of each communication.

As explained below, each of the above types of information can be used to identify previously anonymous Internet users and to reconstruct a detailed history of a subscriber's expressive activity online.

B. The First and Fourth Amendments protect the privacy of Internet users' expressive activities.

It is well established that the First Amendment protects the rights to participate anonymously in expressive activity. The First Amendment guarantee of freedom of speech thus includes the right to speak anonymously; freedom of assembly encompasses the right to associate without giving a name; and the freedom to receive includes the right to listen, watch, and read privately.

The First Amendment right to speak anonymously has a long historical pedigree. See *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995) ("anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent"). This right to anonymity is more than just one form of protected speech; it is part of "our national heritage and tradition." *Watchtower Bible & Tract Soc'y of New York, Inc. v. Village of Stratton*, 536 U.S. 150, 166 (2002).

The Supreme Court first documented the historical value of anonymity in *Talley v. California*, 362 U.S. 60 (1960):

Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. . . . Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes.

Id. at 65.

Protections for anonymous speech are vital to democratic discourse. Allowing dissenters

to shield their identities frees them to express critical, minority views.

Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society.

McIntyre, 514 U.S. at 357 (citation omitted). Fears that their identity may be uncovered, and that they may be persecuted on account of their speech, may prevent minority speakers from speaking at all.

The constitutionally protected freedom of assembly depends upon the freedom to associate without being identified, as the Supreme Court has recognized. *See NAACP v. Alabama*, 357 U.S. 449 (1958), “Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.” *Id.* at 462. *See also Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 558 (1963) (rejecting attempt of state legislative committee to require NAACP to produce membership records); *Sheldon v. Tucker*, 364 U.S. 479, 490 (1960) (striking down state statute requiring that teachers list all association memberships for the previous five years). It is vital that group members may simultaneously identify themselves to one another yet shield their group membership from non-members.

Further, the corollary to the rights to speak and associate, the right to receive speech anonymously, is likewise protected. “It is now well established that the Constitution protects the right to receive information and ideas.” *Stanley v. Georgia*, 394 U.S. 557, 564 (1969), *citing Martin v. City of Struthers*, 319 U.S. 141, 143 (1943) (“This freedom [of speech and press] ... necessarily protects the right to receive”); *Lamont v. Postmaster General*, 381 U.S. 301, 307-08 (1965) (Brennan, J., concurring). Fears of identification based on the speech one invites and receives can have chilling effects upon all parties to a correspondence.

These long-standing rights to anonymity and privacy are critically important to a modern medium of expression, the Internet. As the Supreme Court has recognized, the Internet offers a new and powerful democratic forum in which anyone can become a “pamphleteer” or “a town

crier with a voice that resonates farther than it could from any soapbox.” *Reno v. ACLU*, 521 U.S. at 870. Expansion of the Internet has created countless new opportunities for self-expression and discourse, ranging from the private diary to the multi-million-reader broadcast. The medium hosts tens of millions of dialogues carried out via e-mail publications, Web publications, Usenet Newsgroup message boards, and more, as individuals and associations use the Internet to convey their opinions and ideas whenever they want and to whomever cares to read them.

Many of these of these millions of dialogues occur anonymously or pseudonymously. Most e-mail providers, including free Web-based services such as Yahoo! Mail and Hotmail, allow subscribers to create a e-mail accounts using pseudonyms or to use pseudonymous e-mail addresses, such that subscribers can send messages or join newsletters without disclosing their real names. Subscribers who post to newsgroups hosted on Usenet servers, as well as other message board services such as Yahoo! Groups, are identified only by e-mail address, which again may be pseudonymous. Similarly, hosts of online diaries and journals known as “Weblogs,” such as LiveJournal.com and Blogger.com, allow subscribers to publish their Weblogs pseudonymously, and readers of these weblogs may join the discussion by posting anonymous comments. The widespread anonymity and pseudonymity on the Internet is crucial to its value as an expressive medium.

The *Reno* Court noted that there is “no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.” *Id.* Nor is there any basis for limiting the anonymity and privacy with which people can engage in online speech. The fact that individuals must rely upon intermediaries, including ECSPs, to speak and listen online should not mean that online speech is automatically less free than its offline counterparts. Rather, laws that impair online privacy and anonymity of speech should face the full scrutiny required by the First Amendment offline.

Moreover, Fourth Amendment requirements must be observed with “scrupulous exactitude” when expressional materials are the subject of search or seizure. *Stanford v. Texas*, 379 U.S. 476, 485 (1965); see *Roaden v. Kentucky*, 413 U.S. 496, 501-502 (1973). This concern

is especially great in the NSL context, because “[n]ational security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of ‘ordinary’ crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech.” *United States v. U.S. District Court*, 407 U.S. 297, 313 (1972).

C. Section 2709 unconstitutionally authorizes the FBI to demand a broad array of sensitive records protected by the First and Fourth Amendments.

The Fourth Amendment's "basic purpose . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Municipal Court*, 387 U.S. 523, 528 (1967); *Wolf v. Colorado*, 338 U.S. 25, 27 (1949) ("The security of one's privacy against arbitrary intrusions by the police – which is at the core of the Fourth Amendment – is basic to a free society."). Yet NSLs may be issued completely at the discretion of the FBI Director or his designees, including even special agents in charge of branch offices, without any judicial oversight to guarantee that constitutionally protected records are disclosed only in response to narrowly tailored requests that serve a compelling government interest. Because NSL authority can be used to identify previously anonymous or pseudonymous speakers, readers, and associational activities on the Internet, as detailed below, *Amici* agree with plaintiffs that absent adequate procedural and substantive safeguards protecting these expressive activities from unwarranted exposure, Section 2709 violates the First and Fourth Amendments on its face. See generally Plaintiff's Memorandum in Support of Motion for Summary Judgment, esp. 23-27.

Amici additionally argue that Section 2709 is facially unconstitutional to the extent that it allows, without adequate Fourth Amendment safeguards, the search and seizure of information containing or directly reflecting the contents of communications protected by the Fourth Amendment. See *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that although there is a Fourth Amendment-protected expectation of privacy in the content of a phone call, there is no such expectation regarding the phone number dialed).

In *Smith*, the Supreme Court found that the use by law enforcement of a “pen register” to

record phone numbers dialed by the defendant did not infringe any Fourth Amendment-protected expectation of privacy, “for pen registers do not acquire the *contents* of communications.” *Id.* at 741 (emphasis in original). Indeed,

a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed--a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.

Id., quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977). However, as shown below, records obtainable with an NSL disclose far more than a phone number, revealing the “purport” or meaning, and therefore the constitutionally protected content, of a broad range of Internet communications.

Records obtainable with an NSL can constitute “a profile of an individual’s finances, health, psychology, beliefs, politics, interests, and lifestyle [and] can unveil a person’s anonymous speech and personal associations.” Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002) (footnotes omitted). Section 2709 does not adequately protect the First and Fourth Amendment privacy interests that individuals have in such records, which can disclose a wealth of information about anonymous speakers and readers:

- **The FBI can identify speakers sending e-mail or posting to message boards pseudonymously, e.g., a person petitioning the government via the e-mail address repealPATRIOT@opg.org, or posting a message in support of a political candidate via BushVoter@well.com. The FBI could identify such speakers by requesting from the e-mail provider subscriber records that contain the subscriber’s name.² Even a speaker using a completely anonymous message board**

² To the extent that the e-mail provider is not immediately apparent, two services can be used to discover it: DNS and Whois. First, one uses DNS to discover the designated mail exchanger for the domain in the e-mail address. For example, given the e-mail address wseltzer@eff.org, we see that the domain name is eff.org. Using a DNS client such as nslookup (which comes as part of all Windows, Macintosh and UNIX operating systems) we discover that the (primary) mail exchanger for eff.org is the host mail-dsl.eff.org, which has the IP address 68.120.144.113. Then,

can be identified using the server logs showing the originating IP address and time stamp for each post.³

- **The FBI can identify readers of particular Web sites or pages, and visitors to particular message boards or groups.** ISPs have the capacity to log the Web addresses or other Internet addresses indicating which pages or boards a subscriber visits. Additionally, logs held by the host of the Web site or message board that reflect the IP address of visitors and the time that they visited can be used to identify readers.
- **Web addresses visited by a subscriber can specifically identify everything that subscriber is reading on the Web as well as whatever Web-based communities he associates with.** Many Web addresses directly reflect the content of their corresponding Web pages, e.g., <http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php> points to EFF's analysis of the USA PATRIOT Act, originally published October 31, 2001. However, even Web addresses that contain only unintelligible characters may still point directly to specific pages containing particular speech.
- **Web address logs can give a complete history of a subscriber's Internet search history,** as the Web addresses for the search results pages of many search engines contain the search terms used (e.g., the results of a search for "patriot act")

we can use Whois to discover to whom that IP address has been allocated by the appropriate registrar. (For each continent, there is a different registrar; you can find the right registrar on the Internet Assigned Numbers Authority (IANA) Web site, <<http://www.iana.org/ipaddress/ip-addresses.htm>>). For example, the American Registry for Internet Numbers' (ARIN) Whois service is available on the Web at <<http://ws.arin.net/cgi-bin/whois.pl>>. We can use it to discover that the ISP for the IP address 68.120.144.113 is Pac Bell Internet Services, which could then be served with an NSL.

³ Again, one could use Whois to determine which ISP holds a particular IP address, and then request the identity of the subscriber who was assigned the IP address at the date and time it communicated with the Web site or message board in question.

using Yahoo!'s search engine are displayed at <<http://search.yahoo.com/search?p=patriot+act&ei=UTF-8&fr=fp-tab-web-t&cop=mss&tab=>> (emphasis added)).

- **When a search engine provider is also an ECSP, the search engine's own search history logs may be obtainable via NSL.** Such logs may be correlated with an individual's ISP subscriber information based on the IP address of the party requesting the search. Or, if the user has registered with the search engine provider, whether for search services or other services such as Web-hosting or e-mail service offered by the same ECSP, an NSL need not be served on an ISP at all, as the search provider will already have subscriber information identifying the searching party.
- Similarly, when an Internet user has registered with an ECSP that allows subscribers to access or create message boards or e-mail newsletters, **An NSL to that ECSP can be used to see exactly which message boards or e-mail newsletters the subscriber has created or subscribed to.**
- Conversely, since NSLs can be used to see the e-mail addresses of everyone who corresponds with a particular account, **the FBI can demand the e-mail addresses of every member or subscriber of any particular message board or e-mail newsletter.**
- **An NSL for the e-mail addresses of a subscriber's correspondents can directly identify e-mail newsletters the subscriber receives, and therefore what topics are being discussed and what groups are being associated with, because many e-mail newsletters use e-mail addresses that directly state the name or topic of the list, e.g. Free Israel of Palestine@yahoo.com or Palestine Info Hamas@yahoo.com.**
- **Access to the subscriber's e-mail addresses alone can identify the type of speech and associational activity associated with those addresses. Many e-mail**

users create multiple e-mail address “aliases” for use in different contexts (anyone who registers their own Internet domain, e.g. <www.mydomain.com>, can create multiple aliases, and many e-mail providers offer the same capability, enabling users to create variations of their e-mail addresses by adding to them a plus sign and any additional terms desired). People may use aliases to sort incoming e-mail or to indicate group affiliation. For example, the user of the address anyuser@anyISP.net may subscribe to “CDT Policy Posts,” *amicus* CDT’s e-mail newsletter, using anyuser+CDTPolicyPost@anyISP.net, or may receive *amicus* EFF’s “EFFector” newsletter at anyuser+EFFector@anyISP.net. Similarly, the subscriber might ask personal friends to send to anyuser+personal@anyISP.net while using anyuser+amazon@anyISP.net when registering at Amazon.com. An NSL for a single subscriber’s email addresses can therefore paint a detailed picture of the subscriber’s correspondence and associations.

As the above demonstrates, in addition to identifying previously anonymous readers, speakers, and associations, records obtainable with an NSL include a great deal of information concerning the purport or meaning of communications not at all comparable to the information contained in telephone toll records. In fact, e-mail addresses, Web addresses, IP addresses, and even details such as a downloaded document’s size in bytes may directly contain or be analyzed to identify specific communications content protected by the Fourth Amendment:

- **E-mail addresses are content.** E-mail addresses, as shown above, can themselves contain communicative content in a manner wholly unlike that of numeric phone numbers alone, for example: repealPATRIOT@opg.org, kerryfan@well.com, and anyuser+CDTPolicyPosts@anyISP.net.
- **Web addresses are content.** Web addresses, as discussed above, can directly state the contents of the corresponding Web page. Yet even where they do not, they still directly point to the content on that page, and may also contain additional content such as search terms.

- IP addresses in combination with additional transactional information are content.** In many cases an IP address in combination with other transactional information can specifically identify the particular file downloaded. documents on a Web site have a unique or near-unique size. Therefore, by comparing logs indicating the size of Web pages downloaded from a particular IP address to the size of all of the files available from that IP address, one can identify the specific Web pages that were downloaded. First, using common tools,⁴ one can easily and automatically learn the size of each document on a Web site by downloading them all oneself. This information can then be correlated with the logs showing the details of a particular Internet user's download. Assume, for example, that the FBI obtains records indicating that a surveillance target downloaded a document of size 5,542 bytes from the IP address 206.14.210.244. By checking for files of size 5,542 bytes in it's automatically created, local copy of the Web site hosted at IP address 206.14.210.244 (www.eff.org), the FBI can discover with 100% certainty that the Web page that the target downloaded <http://www.eff.org/Privacy/Surveillance/Terrorism/PATRIOT/pri_act_analysis.pdf>, because that is the only document of that size at the <<http://www.eff.org>> Web site.

To compare the above-described records, which reveal intimate details about a person's speech activities on the Internet, to the sparse information revealed by knowing what phone number called another phone number at what time, is a dramatic extension of the law that the *Smith* court would never have approved.

///

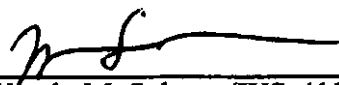
⁴ Examples are the application program wget at <<http://www.gnu.org/software/wget/wget.html>>, and the LWP module for the Perl programming language at <<http://www.cpan.org/authors/id/G/GA/GAAS/libwww-perl-5.79.tar.gz>>.

CONCLUSION

For the foregoing reasons, plaintiffs' motion for summary judgment should be granted.

DATED: May 24, 2004

Respectfully submitted,

By 
Wendy M. Seltzer (WS-4188)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x 125
Facsimile: (415) 436-9993

Kevin S. Bankston

**Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110**

**Attorney for Electronic Frontier Foundation, Online
Policy Group, and Salon Media Group, Inc.**

Nancy Chang

**Center for Constitutional Rights
666 Broadway, 7th Floor
New York, NY 10012**

Attorney for Center for Constitutional Rights

Lara M. Flint

**Center for Democracy and Technology
1634 Eye Street, NW
Suite 1100
Washington, DC 20006**

Attorney for Center for Democracy and Technology

David L. Sobel

**Electronic Privacy Information Center
1718 Connecticut Ave., N.W. Suite 200
Washington, DC 20009**

Attorney for Electronic Privacy Information Center

James W. Butler III

**U.S. Internet Industry Association
815 Connecticut Ave. NW, Suite 620
Washington, DC 20006**

Attorney for U.S. Internet Industry Association

CERTIFICATE OF SERVICE

I hereby certify that, on this 24th day of May, 2004, caused copies of the foregoing BRIEF OF ELECTRONIC FRONTIER FOUNDATION, ET AL., AS AMICUS CURIAE IN SUPPORT OF PLAINTIFFS JOHN DOE AND AMERICAN CIVIL LIBERTIES UNION to be served by Federal Express Overnight Delivery, on counsel of record as follows:

Jameel Jaffer
Ann Beeson
Sharon McGowan
National Legal Department
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004

Arthur N. Eisenberg
New York Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004

Meredith Kotler
Assistant United States Attorney
Southern District of New York
86 Chambers Street, 3rd Floor
New York, NY 10007



Lee Tien

Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333 x 125

Attorney for Electronic Frontier Foundation

May 24, 2004