

ABLE OF A HORL IE

C

A de e C t g LLP . UOP

18 . . 2510, E . . a a . , b. . 99-508, , 201[a]

b a a E
a , a , a a a
E a a , a a ,
a . . a b b a c c ae
a ' a .

I. PRELIMINARY ARGUMENT

a a a 18 . . 2709, a
b b a a a b a
a - a a a , a b
a a a a a a
(), a a a a b a a a
a a a a a b a
b a , a , a b a a a
a . a a a b a
a a a ' ab b a b a a .
a a a a a a a
a a a a . " *Re v. ACLU*, 521 . . 844, 852 (1997).
a a a , - a , a
b a , a b . . 2709 a a a b a
b a , a a a b a a a , -
a a a a a a , a , a
a a , a a a a a a b
a . *A v. C* , a b a a a
a , b b a ' a .

II. HE CHALLENGED THE

2709 E a a (E), ee b . 99-508,
, 201[a]1100 a . 1867 (. 21, 1986) (a 18 . . 2510,),

, a a , a , • a • a ab a¹
•a a •" a .I eD bec c I c. P ac L tg.

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

~~_____~~

~~_____~~

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.
- ~~_____~~
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.

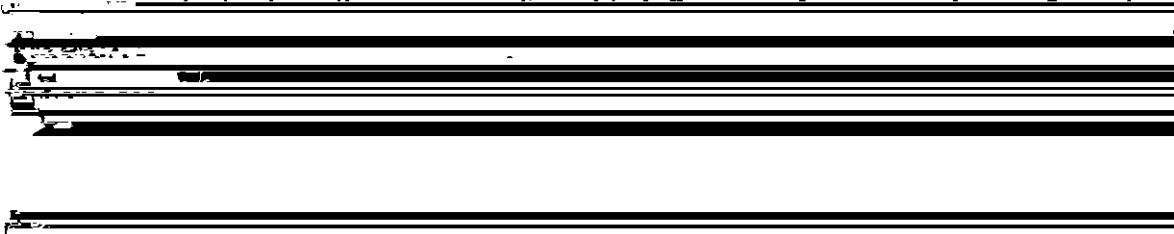
B. The First and Fourth Amendments protect the privacy of Internet users' expressive activities.

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



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); *Shelton v. T. U.*, 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.” *See, e.g.,* *Redden v. C. I.*, 394 U.S. 557, 564 (1969). See *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 ~~_____~~ 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. ~~_____~~ 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 vigilance 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.

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

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

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

requesting from the e-mail provider subscriber records that contain the

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

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

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

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. Establin, J. of Patriot @ ... or Reluctant Life Heroes@...
- 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, ~~names and associations records obtainable with an NSL include a great deal of information~~
~~about the named persons.~~ ~~Some questions not at all comparable to the information~~
contained in telephone toll records. In fact, e-mail addresses, Web addresses, IP addresses, and
~~addresses are content.~~
~~addresses are content.~~

- **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
~~addresses are content.~~
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, such as the size of documents on a Web site, can be used to 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 its 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 is <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.

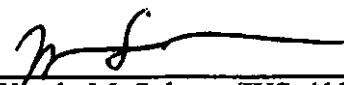
To compare the above-described records, which reveal intimate details about a person's

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 FILING CORPORATION

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

[REDACTED]

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

Meredith Kotler
Assistant United States Attorney

[REDACTED]



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

Attorney for Electronic Frontier Foundation

May 24, 2004