

# 05-0570-cv

---

**UNITED STATES COURT OF APPEALS  
FOR THE SECOND CIRCUIT**

---

**ALBERTO GONZALES, in his official capacity as Attorney General of the United States, ROBERT S. MUELLER III, 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/Appellants,

v.

**JOHN DOE, AMERICAN CIVIL LIBERTIES UNION, and AMERICAN CIVIL LIBERTIES UNION FOUNDATION,**

Plaintiffs/Appellees

---

**ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK**

---

**BRIEF OF ELECTRONIC FRONTIER FOUNDATION, ET AL.,  
IN SUPPORT OF APPELLEES AND AFFIRMATION OF  
JUDGMENT BELOW**

---

Lee Tien  
Kurt B. Opsahl  
Kevin S. Bankston  
Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, CA 94110  
(415) 436-9333  
(415) 436-9993 (fax)

**CORPORATE DISCLOSURE STATEMENT**

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amici Curiae* certify that no publicly held corporation or other publicly held entity owns 10% or more of any *Amicus Curiae*.

Respectfully submitted,

---

Lee Tien  
Kurt B. Opsahl  
Kevin S. Bankston  
Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, CA 94110  
(415) 436-9333  
(415) 436-9993 (fax)

**TABLE OF CONTENTS**

I. INTERESTS OF AMICI.....1

II. PRELIMINARY STATEMENT.....4

III. ARGUMENT .....5

    A. Section 2709 Violates the Constitutional Rights of Internet Users and  
    Service Providers .....5

    B. Section 2709 Applies to a Vast Range of Online Service Providers That  
    Facilitate Free Speech on the Internet .....12

    C. Section 2709 Reaches a Practically Unlimited Array of Records  
    Detailing Internet Users’ Online Speech Activities .....20

IV. CONCLUSION .....26

## TABLE OF AUTHORITIES

### Cases

<i>Andersen Consulting LLP v. UOP</i> , 991 F. Supp. 1041 (N.D. Ill. 1998) .....	19
<i>Bohach v. City of Reno</i> , 932 F. Supp. 1232 (D. Nev. 1996).....	19
<i>Buckley v. American Constitutional Law Found.</i> , 525 U.S. 182 (1999) .....	6, 10
<i>Columbia Ins. Co. v. Seescandy.Com</i> , 185 F.R.D. 573 (N.D. Cal. 1999) .....	9
<i>Davis v. Gracey</i> , 111 F.3d 1472 (10th Cir. 1997) .....	15
<i>Dendrite Int’l, Inc. v Doe</i> , 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001) .....	9, 10
<i>Doe v. 2TheMart.com Inc.</i> , 140 F. Supp. 2d 1088 (W.D. Wash. 2001) .....	8-9
<i>Fischer v. Mt. Olive Lutheran Church</i> , 207 F. Supp. 2d 914 (W.D. Wis. 2002) ....	15
<i>Freedman v. America Online, Inc.</i> , 303 F. Supp. 2d 121 (D. Conn. 2004).....	14
<i>FTC v. Netscape Communications Corp.</i> , 196 F.R.D. 559 (N.D. Cal. 2000) .....	15
<i>Gibson v. Fla. Legislative Investigation Comm.</i> , 372 U.S. 539 (1963).....	7
<i>Guest v. Leis</i> , 255 F.3d 325 (6th Cir. 2001).....	15
<i>Hall v. Earthlink Network, Inc.</i> , 396 F.3d 500 (2nd Cir. 2005).....	15
<i>In re Application of United States for an Order Pursuant to 18 U.S.C. § 2703(D)</i> , 157 F. Supp. 2d 286 (S.D.N.Y. 2001) .....	15
<i>In re Doubleclick Inc. Privacy Litig.</i> , 154 F. Supp. 2d 497 (S.D.N.Y. 2001) .....	14
<i>In re Subpoena Duces Tecum to America Online</i> , 2000 WL 1210372 (Va. Cir. Ct. Jan. 31, 2000) .....	9-10
<i>Klimas v. Comcast</i> , 2003 WL 23472182 (E.D. Mich. 2003) .....	23
<i>Konop v. Hawaiian Airlines, Inc.</i> , 302 F.3d 868 (9th Cir. 2002) .....	15-16
<i>McIntyre v. Ohio Elections Commission</i> , 514 U.S. 334 (1995) .....	6, 7
<i>Melvin v. Doe</i> , 836 A.2d 42 (Pa. 2003) .....	10

<i>NAACP v. Alabama</i> , 357 U.S. 449 (1958).....	7, 8
<i>Recording Indus. Ass’n of America, Inc. v. Verizon Internet Servs., Inc.</i> , 351 F.3d 1229 (D.C. Cir. 2003) .....	10
<i>Reno v. ACLU</i> , 521 U.S. 844 (1997).....	4, 8, 12
<i>Shelton v. Tucker</i> , 364 U.S. 479 (1960).....	8
<i>Sony v. Does 1-40</i> , 326 F. Supp. 2d 556 (S.D.N.Y. 2004) .....	9
<i>Stanley v. Georgia</i> , 394 U.S. 557 (1969).....	7
<i>Steve Jackson Games, Inc. v. United States Secret Service</i> , 36 F.3d 457 (5th Cir. 1994).....	15
<i>Talley v. California</i> , 362 U.S. 60 (1960) .....	6
<i>Tattered Cover, Inc. v. City of Thornton</i> , 44 P.3d 1044 (Colo. 2002).....	7, 8
<i>Theofel v. Farey-Jones</i> , 359 F.3d 1066 (9th Cir. 2004) .....	15
<i>United States v. Monroe</i> , 52 M.J. 326 (C.A.A.F. Mar. 13, 2000) .....	19-20
<i>United States v. Mullins</i> , 992 F.2d 1472 (9th Cir. 1993).....	19
<i>United States v. Perez</i> , 247 F. Supp. 2d 459 (S.D.N.Y. 2003).....	4
<i>United States v. Rumely</i> , 345 U.S. 41 (1953) .....	7, 8
<i>United States v. Steiger</i> , 318 F.3d 1039 (11th Cir. 2003).....	15
<i>United States v. U.S. District Court</i> , 407 U.S. 297 (1972).....	10, 11
<b>Statutes</b>	
18 U.S.C. § 2510(1) .....	14
18 U.S.C. § 2510(12) .....	14
18 U.S.C. § 2510(15) .....	14
18 U.S.C. § 2709.....	passim
18 U.S.C. § 2709(a) .....	5

18 U.S.C. § 2709(b) .....5  
 18 U.S.C. § 2709(c) ..... 5, 21

**Other Authorities**

Preston Galla, *How the Internet Works*  
 (MacMillan Computer Publishing) (1999).....13

**Rules**

Fed. R. Civ. P. 45(c).....9

**Law Review Articles and Treatises**

Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment  
 Privacy*, 75 S. CAL. L. REV. 1083 (2002) .....4  
 U.S. Internet Service Provider Association, *Electronic Evidence Compliance –  
 A Guide for Internet Service Providers*. 18 BERKELEY TECH. L.J. 945 (2003) ...20

The undersigned civil liberties organizations and Internet services providers and associations the Electronic Frontier Foundation, the Center for Constitutional Rights, the Center for Democracy and Technology, the Online Policy Group, Salon Media Group, Inc., Six Apart, Ltd., the U.S. Internet Industry Association, and ZipLip Inc. respectfully submit this brief *amicus curiae* supporting Plaintiffs-Appellees and urge the Court to affirm the decision below. Amici have obtained the consent of all parties.

### **I. 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 CCR is litigating are: *Rasul v. Bush*, 124 S. Ct. 534 (2003); *Humanitarian Law Project v. Gonzales*, Case Nos. CV 98-1971, 03-6107 ABC (C.D. Cal Jul. 28, 2005); and *Turkmen v. Ashcroft*, Case 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 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 20-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 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.

Six Apart, Ltd., based in San Francisco, is the company behind the Movable Type publishing platform, the TypePad personal weblogging service and LiveJournal, an online community organized around personal journals. Six Apart was founded by husband and wife team Ben Trott and Mena G. Trott in 2002, and joined by LiveJournal founder Brad Fitzpatrick early this year. The company is funded by Neoteny Co., Ltd. and August Capital. Six Apart's sole focus is to create simple yet powerful communication tools that enable millions of individuals, institutions and corporations to express, share and connect in ways never before possible. For more information, visit the Six Apart corporate weblog at <http://www.sixapart.com>.

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.

ZipLip Inc., <http://www.ziplip.com>, is a privately held company offering enterprise email archiving and encryption solutions. ZipLip customers include companies subject to government privacy and retention regulations such as Sarbanes Oxley, HIPAA, Gramm Leach Bliley, etc. Until June of this year, ZipLip

hosted their encryption software as an email service used by over 400,000 free and paid subscribers. ZipLip chose to discontinue the hosted service because it could not reasonably assure its email users' privacy and security against government intrusion after passage of the USA PATRIOT Act.

## II. PRELIMINARY STATEMENT

Even when the modern Internet was still in its infancy, the Supreme Court recognized it as a powerful platform for First Amendment activity—a global marketplace of ideas on topics “as diverse as human thought” where anyone could become “pamphleteer” or “a town crier with a voice that resonates farther than it could from any soapbox.” *Reno v. ACLU*, 521 U.S. 844, 852, 870 (1997). The intervening years of unabated growth have only amplified the Internet’s effectiveness as a “vast and largely anonymous distribution and communications network.” *United States v. Perez*, 247 F. Supp. 2d 459, 461 (S.D.N.Y. 2003). However, this medium of unprecedented First Amendment value carries an equally unprecedented threat to liberty, as more online service providers are generating more (and more detailed) records of people’s speech activities than ever before. These records can offer an intimate profile of one’s “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).

National Security Letters (“NSLs”) authorized by 18 U.S.C. § 2709 allow the FBI to secretly obtain these digital dossiers in the form of “subscriber information,” “toll billing records,” and “electronic communication transactional

records” from myriad “electronic communications service provider[s]” (“ECSPs”). 18 U.S.C. § 2709(a). These records are even more revealing of anonymous speech and associational activities than the NAACP’s membership list or a bookstore’s sales records, and are equally deserving of First Amendment protection. Yet NSLs issued under Section 2709 are practically immune from the heightened judicial scrutiny that courts have consistently found necessary to ensure those protections. Instead, they are issued based only on the FBI’s unilateral finding that the records sought “are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities,” and offer neither the served party nor the target any avenue to judicial review. 18 U.S.C. § 2709(b). Section 2709 offers no procedure by which to quash these demands, and binds NSL recipients with a never-ending gag order that has no exception for consulting an attorney. *See* 18 U.S.C. § 2709(c).

This unfettered authority to demand records from ECSPs detailing their subscribers’ speech activities is ripe for abuse, and facially violates the constitutional rights of both ECSPs and their users. *Amici*, representing the interests of a broad range of Internet users and service providers, therefore submit this brief in support of Plaintiffs-Appellees and urge this Court to protect the constitutional rights of Internet users and those who serve them by upholding the District Court’s decision.

### III. ARGUMENT

#### A. Section 2709 Violates the Constitutional Rights of Internet Users and Service Providers

Section 2709 grants the FBI a practically unchecked authority to pierce the

constitutionally-protected anonymity of online speakers, readers and associations. As described in Part C, *infra*, federal agents can wield NSLs to demand a broad range of records detailing Internet users' anonymous speech activities, records in which those users possess a First Amendment-based privacy interest. Yet rather than providing for the heightened evidentiary showing and careful judicial balancing required when the government compels disclosure of such records, the necessary "safeguards of some judicial review... are wholly absent" from Section 2709. SPA-86-87. By this failure, and in addition to violating the constitutional rights of the ECSPs that are subject to NSLs, *see generally* Appellees' Brief at 11-39, Section 2709 facially violates Internet users' First Amendment right to online anonymity.

The right to speak anonymously has an impressive pedigree, as "[e]ven the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names." *Talley v. California*, 362 U.S. 60, 65 (1960); *see also Buckley v. American Constitutional Law Found.*, 525 U.S. 182, 197-200 (1999) (upholding the First Amendment right to speak anonymously by striking down statute requiring that pamphleteers wear name badges). This right is essential to the proper functioning of our democracy: "Anonymity is a shield from the tyranny of the majority," and therefore "exemplifies the purpose" of the First Amendment, which is "to protect unpopular individuals from retaliation...at the hand of an intolerant society." *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 357 (1995). When a law burdens this right, a court must "apply exacting scrutiny" and uphold the law "only if it is narrowly tailored to serve an overriding

state interest.” *Id.* at 347 (citation omitted).

Corollary to the right to speak anonymously is the right to receive speech anonymously, and 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) (citation omitted). That right is unacceptably chilled when the government has unchecked access to reading records: “Once the government can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears,” replaced by the speech-chilling “spectre of a government agent” looking over every reader’s shoulder. *United States v. Rumely*, 345 U.S. 41, 57 (1953) (Douglas, J., concurring); *see also Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1053 (Colo. 2002) (finding that search warrant for bookstore records reflecting a customer’s purchases intruded on customer’s First Amendment right to read anonymously).

The freedom of assembly protected by the First Amendment similarly depends upon the ability to remain anonymous: “Inviolability of privacy in group association may... be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.” *NAACP v. Alabama*, 357 U.S. 449, 462 (1958). Before demanding disclosure of private associational activities, the government must therefore demonstrate a compelling interest “sufficient to justify the deterrent effect which...these disclosures may well have on the free exercise [of the] constitutionally protected right of association.” *Id.* at 463; *see also Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963) (state legislative committee failed to demonstrate an “overriding and

compelling state interest” to justify its demand that NAACP produce membership records); *Shelton v. Tucker*, 364 U.S. 479, 490 (1960) (state’s legitimate inquiry into the fitness of its teachers could not justify statutory requirement that teachers list all association memberships for the previous five years).

Internet service providers, as described in Part C, *infra*, possess a broad range of records analogous to the reading records at issue in *Rumely* and *Tattered Cover*, or the membership rolls and lists in *NAACP* and *Shelton*, and this information along with the identity of anonymous speakers is subject to the same protections afforded in those cases. The Supreme Court has found that there is “no basis for qualifying the level of First Amendment protection that should be applied to this medium,” and the right to speak, read, and associate anonymously applies with full force on the Internet. *Reno v. ACLU*, 521 U.S. at 870. Hence, as the District Court correctly pointed out, “every court that has addressed the issue has held that individual internet subscribers have a right to engage in anonymous internet speech....” SPA-81.

Each of the courts to consider the issue has further found that this First Amendment right requires a heightened evidentiary showing from the subpoenaing party before enforcement of subpoenas to identify anonymous Internet speakers, a requirement that logically and naturally extends to subpoenas that implicate the right to read and associate anonymously. As one court put it: “If Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights.” *Doe v. 2TheMart.com*

*Inc.*, 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001). Secret, unilateral national security demands by the FBI for First Amendment-protected records, issued under the most liberal rules of Section 2709, must be subject to a level of scrutiny at least as strict as that reserved for civil subpoenas, which are not secret and clearly provide served parties with access to a court. *See* Fed. R. Civ. P. 45(c).

In the context of civil subpoenas, the *2TheMart* court found that the Constitution requires a judicial balancing of four factors before a subpoena can be used to identify anonymous Internet speakers:

[W]hether: (1) the subpoena . . . was issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) [adequate] information . . . is unavailable from any other source.”

*Id.* Similarly, all other federal and state courts to address the issue have held that the First Amendment demands a heightened evidentiary showing to justify such subpoenas. In *Sony v. Does 1-40*, 326 F. Supp. 2d 556 (S.D.N.Y. 2004), the court summarized and then applied the most commonly-used criteria:

“(1) a concrete showing of a prima facie claim of actionable harm... (2) specificity of the discovery request ... (3) the absence of alternative means to obtain the subpoenaed information... (4) a central need for the subpoenaed information to advance the claim ... and (5) the party’s expectation of privacy.”

*Id.* at 564-5 (internal citations omitted); *citing Dendrite Int’l, Inc. v Doe*, 775 A.2d 756, 760-61 (N.J. Super. Ct. App. Div. 2001) (denying motion for expedited discovery to obtain identity of ISP subscriber due to failure to establish prima facie defamation claim); *Columbia Ins. Co. v. Seescandy.Com*, 185 F.R.D. 573, 577-81 (N.D. Cal. 1999); *In re Subpoena Duces Tecum to America Online*, 2000 WL

1210372, at \*8 (Va. Cir. Ct. Jan. 31, 2000), *rev'd on other grounds, America Online, Inc. v. Anonymous Publicly Traded Co.*, 261 Va. 350, 542 S.E.2d 377 (2001); and *Recording Indus. Ass'n of America, Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229 (D.C. Cir. 2003).

The First Amendment requires courts to carefully weigh whether the necessary evidentiary showing has been met. “[T]he right to anonymous free speech... falls within the class of rights that are too important to be denied review,” *Melvin v. Doe*, 836 A.2d 42, 50 (Pa. 2003). Thus, courts must “be vigilant... [and] guard against undue hindrances to political conversations and the exchange of ideas.” *Id.* at 1095 (quoting *Buckley*, 525 U.S. at 192). This vigilant review “must be undertaken and analyzed on a case-by-case basis,” where the court’s “guiding principle is a result based on a meaningful analysis and a proper balancing of the equities and rights at issue.” *Dendrite*, 775 A.2d at 760-761.

Such a careful case-by-case balancing of rights cannot constitutionally be left to the FBI’s sole discretion, particularly in the context of national security investigations. As the Supreme Court has warned,

National 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). The dangerous vagueness of the government’s “domestic security” interest demands judicial checks against abuse, or else the Executive would be free to unilaterally declare “draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists to be a

clear and present danger to the structure or existence of the Government.” *Id.* (internal quotation omitted). Similarly, every “national security”-based demand for First Amendment-protected records must be effectively subject to judicial review. Heightened judicial scrutiny is the only constitutionally meaningful check to prevent the Executive from secretly and illegally using NSLs to gather information about political adversaries and advocates for unpopular causes.

As the District Court correctly held, the FBI cannot be entrusted to regulate itself in such matters. Only a court can strike the appropriate balance between the government’s interests and the First Amendment privacy of Internet users. SPA-80. Only a court can properly assess whether the government has met a heightened evidentiary burden that justifies encroachment on First Amendment rights. This Court need not define the contours of the specific balancing to be applied when such national security authorities are subject to judicial review, but it is undeniable that those powers must be subject to *some* level judicial scrutiny. Yet Section 2709, both on its face and as applied, fails to provide ECSPs or their customers with effective access to any judicial review.

*Amici* therefore agree with Plaintiffs-Appellees that Section 2709 facially violates the First Amendment rights of online speakers, by allowing the FBI unchecked access to a breathtaking range of ECSP records revealing Internet users’ anonymous speech activities. As described in detail below, it is inevitable that online speakers must reveal some information about themselves to their ECSPs in order to take advantage of the “vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers.”

*Reno v. ACLU*, 521 U.S. at 853. That inevitable fact, however, does not eliminate users' First Amendment right to online anonymity. Rather, as the District Court correctly found, users' First Amendment privacy interest in their ECSPs' records only reinforces the conclusion that Section 2709 unconstitutionally fails to provide ECSPs with a meaningful opportunity for judicial review, whether to protect their own rights or the rights of their customers. SPA-77.

*Amici* therefore also agree with the District Court's conclusion that Section 2709 violates the First and Fourth Amendment rights of ECSPs by effectively immunizing the FBI's forever-secret demands for records from any judicial process.<sup>1</sup> SPA-76, 109. As explained in more detail below, the NSL authority threatens the constitutional rights of countless ECSPs offering a broad range of Internet services, and through them, endangers the First Amendment rights of every Internet user.

**B. Section 2709 Applies to a Vast Range of Online Service Providers That Facilitate Free Speech on the Internet**

In exercising their speech rights online, Internet users necessarily must rely on a variety of third parties offering a wide array of services, all or most of which are covered by Section 2709. The Internet is not a single service that can be packaged and sold by a single entity, but rather a global network of individual computers and computer networks over which an ever-changing variety of communications services can be offered, the most obvious being the World Wide

---

<sup>1</sup> In addition to these constitutional violations, Section 2709 additionally burdens ECSPs by failing to provide for reimbursement of their costs in complying with NSLs.

Web (“Web”) and e-mail.<sup>2</sup> A-41. Therefore, an Internet user’s Internet service provider (“ISP”), which connects the user’s own computer or private network to that global network, is usually only the first necessary intermediary an Internet user will encounter. A-42. And although ISPs often bundle some services, such as an e-mail account or Web hosting, with their provision of Internet access, those same services and myriad others are also available from different service providers across the Internet. A-41-42. As described in Part C, *infra*, these varied, non-ISP

---

<sup>2</sup> An expanded discussion of the Internet’s basic technical 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 computer language, 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).

These additional protocols use their own types of addresses, apart from IP 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@emailprovider.com](mailto:user@emailprovider.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.

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 SMTP (e-mail) is assigned to port 25.

service providers all possess records that could be used to unmask anonymous speakers, identify anonymous readers, and reveal private associations, particularly if combined with subscriber account information from an ISP. And most if not all of these service providers, ISPs and non-ISPs alike, are subject to NSLs.

Any “electronic communications service provider,” whether small or large, public or private, commercial or non-profit, is subject to the NSL authority. 18 U.S.C. § 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). A wire communication is, essentially, any transmission of the human voice that isn’t broadcast to the public. *See* 18 U.S.C. § 2510(1). The definition of an “electronic communication” includes “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,” so long as it is not also a wire communication.<sup>3</sup> 18 U.S.C. § 2510(12).

Applying these definitions to the Internet, it is well-settled that ISPs qualify as ECSPs. *See In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 511 n. 20 (S.D.N.Y. 2001) (“ISPs such as America Online, Juno and UUNet, as well as, perhaps, the telecommunications companies whose cables and phone lines carry the traffic” are ECSPs); *Freedman v. America Online, Inc.*, 303 F. Supp. 2d 121, 124 (D. Conn. 2004) (automatically equating ECSPs with ISPs such as America

---

<sup>3</sup> Notably, a significant portion of wire communications traffic now occurs over the Internet. A-41.

Online); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004) (Netgate, an ISP that also provided e-mail service, was ECSP); *Hall v. Earthlink Network, Inc.*, 396 F.3d 500, 502 (2nd Cir. 2005) (ISP Earthlink, which also provided e-mail service, was ECSP). ISPs that provide Internet access to other ISPs—e.g., “UUNet, which provided ‘backbone’ Internet services to Earthlink,” *id.* at \*1—are also ECSPs, as they offer consumer ISPs like Earthlink the ability to send and receive the communications of their customers.

However, one need not be an ISP (or the ISP of an ISP) to be subject to an NSL. For example, e-mail service providers that are not themselves ISPs are still ECSPs. *See, e.g., In re Application of United States for an Order Pursuant to 18 U.S.C. § 2703(D)*, 157 F. Supp. 2d 286, 289 (S.D.N.Y. 2001) (finding that Microsoft provides electronic communications service through its Web-based e-mail service Hotmail); *Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp. 2d 914, 925 (W.D. Wis. 2002) (same); *FTC v. Netscape Communications Corp.*, 196 F.R.D. 559, 560 (N.D. Cal. 2000) (same for Netscape’s Web-based e-mail service).

Similarly, even though not offering Internet access directly, providers of computer “bulletin board services” (“BBSs”) that allow users to post electronic messages are ECSPs. *See United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003), *cert. denied*, 538 U.S. 1051 (2003); *Guest v. Leis*, 255 F.3d 325, 338 (6th Cir. 2001); *Davis v. Gracey*, 111 F.3d 1472, 1484 (10th Cir. 1997); and *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 458, 462 (5th Cir. 1994). Companies that host users’ Web sites or pages or allow users to post messages to the Web are also presumably ECSPs. *See Konop v. Hawaiian Airlines*,

*Inc.*, 302 F.3d 868, 879-80 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003) (assuming that host of Web-based message board was ECSP).

Practically any online service that allows users to receive, send or publish a communication over the Internet could be classified as an ECSP, including many free services that allow or even encourage anonymous or pseudonymous use:

- **Free Web-based e-mail services** from providers such as Yahoo (<http://mail.yahoo.com>), Microsoft (<http://www.hotmail.com>), and Google (<http://www.gmail.com>), where users can create pseudonymous e-mail addresses for sending and receiving messages.
- **Free Web hosting services** such as Yahoo's Geocities (<http://geocities.yahoo.com>) and AOL's Hometown service (<http://hometown.aol.com>), which allow pseudonymous users to create their own Web pages and publish whatever they choose.
- **Free Web log or "blog" hosting services** such as Google's Blogger (<http://www.blogger.com>), and paid blog hosts such as *amicus* Six Apart's TypePad (<http://www.typepad.com>). Blog hosts are much like regular Web hosts, except that they also provide access to specialized "blogging" software that makes it especially easy for customers to post regular updates to their Web pages. Blogs are often used as personal platforms for political news and opinion, *see, e.g.*, the conservative blog InstaPundit.com, the liberal TalkingPointsMemo.com, or the bipartisan political gossip site Wonkette.com. Some blog services, like Six Apart's online diary service LiveJournal.com, allow the user to publish a private blog that can only be

viewed by other subscribers that the author has designated.

- **Free Web-based bulletin board services** offered by companies like Google, Yahoo, and Microsoft (<http://groups.google.com>, <http://groups.yahoo.com>, and <http://groups.msn.com>), where users can pseudonymously create or join public bulletin boards on any topic, or create boards that are only accessible to other members of the service that the creator has designated, any of whom may also be pseudonymous.
- **Free community message boards** like Craigslist (<http://www.craigslist.com>), where users in every major U.S. city (and many non-U.S. cities) can pseudonymously post classified ads of all stripes and participate in local community discussion boards on a variety of topics.
- **Online bookstores and others that allow users to post ratings and reviews on the Web**, including online bookstore Amazon.com and online DVD rental store Netflix.com. On these sites, countless readers have been able to post pseudonymous reviews of nearly every book or movie that is available to the public.
- **Free online dating services** like those offered by *amicus* Salon, Yahoo, and Gay.com (<http://personals.salon.com>, <http://personals.yahoo.com>, and <http://personals.gay.com>), where people can pseudonymously publish a personal profile with pictures, and exchange private messages with others who have posted personal ads on the same service.
- **Picture-sharing sites** such as the Yahoo-owned Flickr.com, which has been able to build an unimaginably broad library of digital photographs that users

have submitted, categorized, and rated. Users can choose to publish pictures to the world or only share them with other friends on the service, and can do both pseudonymously. Such sites are a vibrant new source of citizen photojournalism. *See, e.g., PCWorld.com, Flickr Pics Capture London Terror, at <http://www.pcmag.com/article2/0,1895,1834859,00.asp> (Jul. 7, 2005).*

- **Personalized news pages** like those offered by Yahoo (<http://my.yahoo.com>) or NewsIsFree.com, where users can register pseudonymously and preselect the types and topics of information they would like to see when they log onto the home page, including constantly-updated newsfeeds showing the latest news stories on preselected topics or the latest blog posts from favorite bloggers.
- **Other Web sites that allow visitors to send messages**, such as *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 civil liberties issues.

As shown above, the Web alone<sup>4</sup> offers a wide range of services with political and associational qualities in which individuals can participate anonymously. It is also clear that a few key “mega-providers”—like AOL, Google, Microsoft and Yahoo—have developed complete suites of online services and are

---

<sup>4</sup> Of course, the Web is merely one of the many modes of Internet communication. Internet communications take place in a variety of forms, including e-mail, discussion groups over Usenet, moderated and unmoderated mailing lists, multi-player game spaces, chat systems, and other file transfer and retrieval mechanisms, the providers of which would all appear to be covered under Section 2709. A-41.

becoming the primary Internet “portals” for a vast amount of online activity. For example, in addition to using Yahoo’s search engine (<http://www.yahoo.com>), an Internet user may rely on Yahoo for Internet access, e-mail, instant text messaging, Web hosting, group bulletin boards, social networking and dating, online shopping and job-hunting, managing a personal address book and calendar, and any of the other services catalogued at <http://help.yahoo.com>. Google similarly offers an equally broad range of services (*see* <http://www.google.com/intl/en/options>). These mega-providers, with access to almost every variety of communications record, offer convenient “one-stop shopping” for FBI agents armed with NSLs, compounding their reach and intrusiveness.

Just as NSLs can be used against the biggest providers that serve the public, so to can they be used against the smallest or most private. The “electronic communications service” definition is not limited to entities providing services to the general public. Thus any corporate office, government office, school, library, or other organization that offers its employees, students or members the means to communicate over the Internet or any internal computer network may be an ECSP. *See, e.g., United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993), *cert. denied*, *Mullins v. U.S.*, 510 U.S. 994 (1993) (airline that provided travel agents with computerized travel reservation system accessed through separate computer terminals was ECSP); *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1042 (N.D. Ill. 1998) (consulting firm Andersen, which had internal e-mail system, was ECSP); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (city that provided pager service to its police officers was ECSP); *United States v. Monroe*,

52 M.J. 326 (C.A.A.F. Mar. 13, 2000) (U.S. Air Force, which provided e-mail accounts for official business, was ECSP). Even a local Starbucks coffee shop that provides wireless Internet access to its customers, A-45, or an individual that runs a home wireless network allowing visitors and passersby to access the Internet, could be subject to an NSL.

Rather than covering only traditional ISPs, then, Section 2709 impacts the First and Fourth Amendment rights of tens if not hundreds of thousands of companies, individuals, and organizations, and provides countless points of attack against Internet users' First Amendment rights. The number and variety of such services is steadily growing, and the records kept by those ECSPs about their users' online activities will also increase in number and granularity as computer networking and storage technology becomes cheaper and more powerful.

**C. Section 2709 Reaches a Practically Unlimited Array of Records Detailing Internet Users' Online Speech Activities**

The varied multitudes of ECSPs subject to Section 2709 possess records that, as described below, can be used alone or in combination to unmask anonymous speakers and reveal private reading habits and associations. Yet Section 2709 is a particularly "awkward" provision for ECSPs because it uses wholly undefined terms to describe which of those records the FBI may demand, i.e., "subscriber information and toll billing records information, or electronic communication transactional records," including "name, address, length of service, and local and long distance toll billing records." 18 U.S.C. § 2709; *see also* 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 had the opportunity to consider the scope of these phrases, such as “toll billing records” and “electronic communication transactional records,” that appear nowhere else in the U.S. Code, presumably because no ECSP has ever had an effective opportunity to seek judicial review of those terms.

Insofar as the types of records obtainable with an NSL are in doubt, the ECSPs served with NSLs are in a poor position to properly protect their interests and those of their subscribers. Each NSL is accompanied by a gag order prohibiting the ECSP from ever revealing the demand was made, see 18 U.S.C. § 2709(c). 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. Such vague terms could easily be construed to apply to any and every type of record the ECSP has about its users, including:

- Subscriber account information such as name, physical address, phone number, length of service and types of service subscribed to, and the means and source of payment for the service, including any credit card or bank numbers.
- Connection logs showing when the subscriber connected to and disconnected from the ECSP’s service.
- The subscriber’s e-mail address(es) or other username(s), often-pseudonymous titles that the subscriber uses when logging into the service, or when publishing or otherwise communicating through the service.
- Logs of e-mail “header” information that include the e-mail address of the

sender and recipient(s), as well as information about when each e-mail 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 by the subscriber's ISP, and the IP addresses of other Internet-connected computers that the subscriber sent to or received from.
- Server logs showing the source (i.e., IP address) of requests to view or post to a particular Web page, or otherwise access any online service.
- 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, instant message).
- The size and length of each communication, and the time it occurred.

*See generally* A-45-48. Alone and in combination, this information can be used to identify previously anonymous Internet users or reconstruct a detailed history of their expressive activity online: what they said, what they read, and with whom they associated.

NSLs are thus powerful tools for revealing anonymous Internet speakers without judicial oversight. For example, consider a controversial message board poster or political blogger who publishes news and opinion about the administration's antiterrorism policies under a pseudonym. If the ECSP has personal information about the subscriber—for example, if the user registered with the blog host or message board host using a real name, or had to give identifying

information because it was necessary to purchase services or products—the pseudonymous speaker could be immediately identified with a single NSL for subscriber information. Even if the service lacked such subscriber information, logs showing the user’s IP address when accessing the service could be traced back to the user’s ISP,<sup>5</sup> and a second NSL could be issued to that ISP for identifying information.

Cloaked in secrecy and without judicial review, the FBI might also use an NSL to discover the Web sites and message boards a particular user reads or posts to. ISPs have the capacity to log the Web addresses and other Internet addresses indicating which pages or boards a subscriber visits, A-47, and have been known to do so without their subscribers’ knowledge. *See Klimas v. Comcast*, 2003 WL 23472182, \*1 (E.D. Mich. 2003). ECSPs other than ISPs may also have logs identifying every Web page visited, by virtue of services that allow users to store that history for future personal reference (e.g., Amazon’s A9 search toolbar, available at <http://toolbar.A9.com>) or services that require the user to share such information in order for the service to function, such as Google’s Web Accelerator (<http://webaccelerator.google.com>) and some features available in Google’s search

---

<sup>5</sup> This is accomplished using a tool called Whois, offered for free by a variety of entities. 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>. Anyone can type any IP address into a form and be told what ISP currently uses IP addressees in that range of numbers. So, for example, an NSL could be served on a particular Web service to see logs identifying what IP addresses were used to access it at what times. Those IP addresses could be plugged into Whois to identify the relevant ISPs, who could then be served with NSLs demanding the account information of those subscribers using the relevant IP addresses at the relevant times.

toolbar (<http://toolbar.google.com>).

This vast trove of data opens users of these services to the inspection of their most private thoughts, their interests and passions, their political beliefs and medical ailments. The Web addresses a person visits can specifically identify everything that person 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, or indicate the organization that publishes it. For example, [http://www.eff.org/Privacy/Surveillance/Terrorism/20011031\\_eff\\_usa\\_patriot\\_analysis.php](http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php) clearly points to EFF's analysis of the USA PATRIOT Act, originally published October 31, 2001. However, even when Web addresses contain only unintelligible characters, the FBI can simply use the address itself to see the content of the relevant Web site or bulletin board and identify what the target was reading and with whom he was associating.<sup>6</sup>

Web address logs can also give a complete history of a subscriber's Internet search history, as the Web addresses for the search results pages of most search engines contain the search terms used (e.g., the results of a search for "patriot act" using Yahoo!'s search engine are displayed at <http://search.yahoo.com/search?p=patriot+act&sm=Yahoo%21+Search&fr=FP-tab-web->

---

<sup>6</sup> Even when Web address logs are unavailable, IP address logs in combination with other transactional information can specifically identify the particular Web pages an Internet user is reading.

The Web pages that can be downloaded from a particular IP address often are unique or near-unique in 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.

t&toggle=1&cop=&ei=UTF-8 (emphasis added)).

A person's search history may be vulnerable to NSLs even if there are no Web address logs to examine: if the search provider is also an ECSP, federal agents could demand its own search history logs. Such logs could be correlated with IP logs, or, if the user has registered with the provider for search or other services using personally identifying information, could be directly matched to identity. 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 could be used to see exactly which political message boards or e-mail newsletters the subscriber has created or subscribed to.

E-mail header information that the FBI can demand with an NSL is equally revealing of one's associations. The government could use an NSL to demand the e-mail addresses of everyone who has ever corresponded with the targeted account. Furthermore, 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 the subscriber associates with. That is 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@yahoogroups.com` or `Palestine_Info_Hamas@yahoogroups.com`, or EFF's weekly newsletter the `EFFector`, sent via `effector@eff.org`. Conversely, the FBI could demand the e-mail addresses of every member or subscriber of a particular message board or e-mail newsletter service.

Considering e-mail and Web-based services alone—only two of the many

kinds of communications services available online—it is obvious that the information that the FBI can secretly and unilaterally demand with an NSL provides a nearly-complete roadmap of Internet users’ anonymous speech activities. Yet Section 2709 fails to effectively provide any judicial review of the FBI’s secret demands, whereby ECSPs could assert the First Amendment rights of their users along with their own First and Fourth Amendment rights. Consequently, Section 2709 facially violates these constitutional rights of both ECSPs and their users.

#### **IV. CONCLUSION**

For the foregoing reasons, the government’s appeal should be denied and the District Court’s ruling affirmed.

Respectfully submitted,

---

Lee Tien  
Kurt B. Opsahl  
Kevin S. Bankston  
Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, CA 94110  
(415) 436-9333  
(415) 436-9993 (fax)