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

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

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Law Review Articles and Treatises

The undersigned civil liberties organizations and Internet services providers and associations the Electronic Frontier

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

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.

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

Inc., 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001). Secret, unilateral national

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

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.[1] 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

[1] In addition to these constitutional violations, Secti

Web ("Web") and e-mail.[2] 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

[2] 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 Pubms own-tem

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-

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 Inte

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:

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 communitfc membersess5S1 gsBTTT4 1 Tfs5-3site

http:/www.crigslistn.c m) w)-1(here userse)TJ42 0 TD0.001 Tc0.

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),

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,vitif ECSv95rful.

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

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 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.[6]

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-

[6] 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)