

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Nos. 05-50410, 05-50493

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

MARK STEPHEN FORRESTER
Defendant-Appellant.

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

DENNIS LOUIS ALBA,
Defendant-Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF CALIFORNIA
HONORABLE THOMAS J. WHELAN

**AMICUS BRIEF OF AMERICAN CIVIL LIBERTIES UNION
FOUNDATION, AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF SAN DIEGO AND IMPERIAL COUNTIES,
AMERICAN BOOKSELLERS FOUNDATION FOR FREE
EXPRESSION, AND ELECTRONIC FRONTIER FOUNDATION IN
SUPPORT OF APPELLANT ALBA'S PETITION FOR REHEARING
AND SUGGESTION FOR REHEARING EN BANC**

Catherine Crump
Aden J. Fine
American Civil Liberties Union
Foundation
125 Broad Street, 17th Floor
New York, NY 10004-2400
(212) 519-7806
Attorneys for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

The American Civil Liberties Union Foundation, American Civil Liberties Union Foundation of San Diego & Imperial Counties, American Booksellers Foundation for Free Expression, and the Electronic Frontier Foundation do not have any parent corporations, and no publicly held company owns ten percent or more of stock in any of these *amici*.

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
STATEMENT OF INTEREST	iii
RULE 35(b) STATEMENT	1
BACKGROUND.....	3
REASONS FOR GRANTING THE PETITION	6
I. The Panel’s Conclusion That Individuals Have No Expectation of Privacy in the IP Addresses of the Web Sites They Read Conflicts with Supreme Court Precedent and Ignores Societal Expectations.....	6
II. The Panel’s Sweeping Dicta Eviscerates Fourth Amendment Protection for All Internet Communications and Conflicts With Supreme Court Precedent	14
CONCLUSION	15
CERTIFICATE OF COMPLIANCE.....	16
PROOF OF SERVICE	17

TABLE OF AUTHORITIES

Cases

<i>Ex parte Jackson</i> , 96 U.S. 727 (1877)	3
<i>Georgia v. Randolph</i> , 547 U.S. 103 (2006)	5
<i>Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.</i> , 26 Media L. Rep. (BNA) 1599 (D.D.C. 1998)	11
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	<i>passim</i>
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001)	5
<i>Reno v. ACLU</i> , 521 U.S. 844 (1997).....	3, 6, 12
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979)	<i>passim</i>
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965)	5
<i>Tattered Cover, Inc. v. City of Thornton</i> , 44 P.3d 1044 (Colo. 2002).....	11

STATEMENT OF INTEREST¹

The American Civil Liberties Union Foundation (“ACLU”) is a nationwide, nonprofit, nonpartisan organization with over 500,000 members dedicated to the principles of liberty and equality embodied in the U.S. Constitution. The ACLU of San Diego and Imperial Counties is devoted to the preservation and advancement of civil liberties through public education and litigation. The protection of privacy as guaranteed by the Fourth Amendment is an area of special concern to both organizations.

The American Booksellers Foundation for Free Expression (“ABFFE”) is the bookseller’s voice in the fight against censorship. Founded by the American Booksellers Association in 1990, ABFFE’s mission is to promote and protect the free exchange of ideas, particularly those contained in books, by opposing restrictions on the freedom of speech. In recent years, ABFFE has strongly defended reader privacy—the right of Americans to read without the fear that the government is looking over their shoulders.

The Electronic Frontier Foundation (“EFF”) is a non-profit, member-supported civil liberties organization working to protect free speech and privacy rights in the online world. As part of that mission, EFF has served as

¹ All parties have consented to the filing of this brief.

counsel or amicus in key cases addressing electronic privacy statutes and the Fourth Amendment as applied to the Internet and other new technologies. With more than 12,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age. EFF also publishes a comprehensive archive of digital civil liberties information at one of the most linked-to Web sites in the world, www.eff.org.

RULE 35(b) STATEMENT

Rehearing or rehearing en banc is warranted because this case involves a question of exceptional importance: do individuals have a reasonable expectation of privacy in the IP addresses of the Web sites they read? The answer to this question--presented to a circuit court for the first time--will have a major impact on the ability of Americans to read and view materials freely on the Internet, unconstrained by the fear of government surveillance.

Millions of Americans read Web sites every day. The information they seek is diverse and often personal. The IP addresses of the Web sites an individual reads provide a detailed picture of, among other things, that person's religious and political beliefs, relationship status and sexual interests, health concerns, personal and career aspirations, and hobbies and general interests.

The panel erred in concluding that the government can collect the IP addresses of the Web sites an individual reads without implicating the Fourth Amendment on the ground that IP addresses of Web sites do not contain content. That IP addresses reveal communications content is apparent from the factual record in this case, as the government relied on the Web sites Alba read to obtain a warrant for more invasive surveillance. It is

also clear as a general matter. IP addresses can reveal the subjects of what the computer owner is reading--in the instant case chemistry and its effect on the body. In other words, they reveal subject matter content. The panel's decision is also contrary to the general societal expectation that individuals' Web viewing habits are private. This Court should grant rehearing or rehearing en banc and hold that individuals have a reasonable expectation of privacy in the Web sites they read, and that the government cannot obtain the IP addresses of the Web sites individuals read without a warrant.

The panel also erred in reasoning that individuals have no Fourth Amendment interest in this information because they "should know that . . . IP addresses are accessed through the equipment of their Internet service provider and other third parties." Slip op. at 8083. If this sweeping statement is left undisturbed, it would justify warrantless government surveillance of *all* Internet communications. All Internet communications are, by definition, "accessed through the equipment of" an Internet service provider. Under the panel's reasoning, that would mean that there is no expectation of privacy in any Internet speech, and that the government could intercept and monitor the content of all Internet speech without a warrant. Such a ruling is directly precluded by the Supreme Court's decision in *Katz v. United States*, 389 U.S. 347, 352 (1967), in which the Court held that

individuals have a reasonable expectation of privacy in the content of their communications, and *Reno v. ACLU*, 521 U.S. 844 (1997), which made clear that speech on the Internet is entitled to the same protections as all other speech. At minimum, the panel opinion should be amended to clarify that the government cannot intercept or monitor information containing communications content without a warrant.

BACKGROUND

The Supreme Court has consistently held that the government needs a warrant to intercept and monitor the content of private communications. The Court's first opportunity to consider this question arose in the context of traditional mail. *Ex parte Jackson*, 96 U.S. 727, 733 (1877) ("Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection . . . as if they were retained by the parties forwarding them in their own domiciles."). More recently, the Court held that individuals have a reasonable expectation of privacy in the content of their telephone calls. *Katz*, 389 U.S. at 352. The Court wrote that an individual placing a telephone call "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." *Id.* That is so even though "[t]he telephone conversation itself must be electronically transmitted by telephone company equipment, and may be

recorded or overheard by the use of other company equipment.” *Smith v. Maryland*, 442 U.S. 735, 746 (1979) (Stewart, J., dissenting). The *Katz* Court concluded that “[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.” *Katz*, 389 U.S. at 352.

The Court’s decision in *Smith* reaffirmed the Fourth Amendment’s protection of communications content. In *Smith*, the Court held that use of a pen register to obtain only the telephone numbers an individual dials does not violate the Fourth Amendment. *Smith*, 442 U.S. at 736. The Court made clear that its holding that no warrant was required for the use of a pen register was limited only to that situation where content was not revealed:

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

Id. (quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977)).²

The narrowness of the *Smith* decision was mandated by the Court’s

² Amici believe the Court erred in concluding that telephone numbers do not implicate a privacy interest. Among other things, a list of the telephone numbers an individual dials can reveal much about that person’s associations.

prior decision in *Katz*. In *Katz*, the Court protected the contents of telephone calls, even though they were transmitted through a third party's network, because of the societal expectation that telephone conversations are private. *Katz*, 389 U.S. at 352. Since *Katz*, the Court has continued to rely on societal expectations when analyzing the application of the Fourth Amendment. *See, e.g., Georgia v. Randolph*, 547 U.S. 103 (2006) (finding search based on spouse's consent unreasonable based on "widely shared social expectations" and "commonly held understanding[s]" regarding the authority of co-inhabitants). Further, the Court has emphasized that the government should not be able to intrude into core Fourth Amendment protections because of changing technology. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (recognizing that technological advances must not be allowed to erode society's expectation in "that degree of privacy against government that existed when the Fourth Amendment was adopted"). That is especially the case where First Amendment rights are at issue. *See, e.g., Stanford v. Texas*, 379 U.S. 476, 485 (1965) ("[T]he constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain.").

REASONS FOR GRANTING THE PETITION

This case presents the first opportunity for this Court to consider how to extend the protections of the Fourth Amendment to the new context of Internet speech. In *Reno v. ACLU*, the Supreme Court observed that “the content on the Internet is as diverse as human thought” and held that Internet speech is fully protected under the First Amendment. 521 U.S. at 870. The ability to read the Web free from the prospect of government surveillance is an important reason for the breadth and diversity of thought on the Web. This Court should find that Internet communications are fully protected under the Fourth Amendment as well. Just as the Supreme Court extended the Fourth Amendment’s protection to the content transmitted over the new medium of the telephone in *Katz*, this Court should extend the Fourth Amendment to cover the Web sites an individual views on the Internet.

I. The Panel’s Conclusion That Individuals Have No Expectation of Privacy in the IP Addresses of the Web Sites They Read Conflicts with Supreme Court Precedent and Ignores Societal Expectations.

Analogizing to *Smith*, the panel concluded that Web site IP addresses viewed are not protected by the Fourth Amendment because they do not reveal the content of communications:

IP addresses constitute addressing information and reveal no more about the underlying contents of communication than do phone numbers. When the government learns the phone numbers a person has dialed, it may be able to determine the

persons or entities to which the numbers correspond, but it does not know what was said in the actual conversations. Similarly, when the government obtains . . . the IP addresses of websites visited, it does not find out the . . . particular pages on the websites the persons viewed. At best, the government may make educated guesses about what was . . . viewed on the websites based on its knowledge of the . . . IP addresses--but this is no different from speculation on the contents of a phone conversation on the basis of the identity of the person or entity that was dialed.

Slip op. at 8084.

The panel suggests that if the information the government collected had been more revealing, it might have applied more rigorous scrutiny:

Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators (“URL”) of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person’s Internet activity.

Slip op. at 8084 n.6.

This reasoning is flawed in at least three respects. First, it takes an overly limited view of what constitutes communications content. Even though the panel acknowledges that Web site IP addresses often reveal the specific Web sites an individual reads, it holds that the fact that the government has to make “educated guesses” about what “particular pages on the websites the persons viewed” exempts Web site IP addresses from the Fourth Amendment’s coverage. That is not the law. The Supreme Court has

made clear that law enforcement must obtain a warrant *whenever* it intercepts or monitors the content of any communication. *Katz*, 389 U.S. at 352. The fact that the government learned the Web site viewed (i.e. www.MinutemanProject.com, www.Playboy.com) instead of the specific Web page (i.e www.MinutemanProject.com/organization/about_us.asp, http://www.Playboy.com/girls/index.html) is legally irrelevant. The question is not at what level of generality the government's surveillance reveals communications content, but rather whether it reveals content information *at all*. Knowing that a person has viewed a particular Web site reveals what the person looked at--i.e., content. Knowing further information about which additional pages on that site have been viewed would simply provide more content information.

Second, Web site IP addresses do reveal a great deal of information about communications content. The government's own affidavit demonstrates that its surveillance of Alba's Web usage revealed communications content. Affidavit of Gregory D. Coffey, Special Agent, United States Drug Enforcement Administration, July 6, 2001, Record at 50524-50568 (hereinafter "Coffey Affidavit").³

³ The government first used its purported pen register analog to collect information about Alba's Internet usage, and then sought a warrant based on

The government explained that its surveillance of Alba's Web usage "provides a road map of where the user of the Target Account goes while on-line by capturing the IP addresses accessed by the Target Account."

Coffey Affidavit at 26, Record at 50549. The affidavit explained:

An analysis of data obtained from the "mirror port" reveals that the Target Account accessed the following websites: ChemFinder.com on May 12 and 14, 2001; ChemStore.com on May 12, 2001; several Chinese chemical and medical sites on May 10, 2001; and GalladeChem.com on June 20, 2001.

Id. at 29; Record at 50552. This is only a small fraction of the government's surveillance, but even this limited sample reveals the content of Alba's Web reading. It indicates that he read about the topics of chemistry and medicine. Unlike the telephone numbers in *Smith*, Web site IP addresses do not merely indicate *who* an individual may have contacted. They indicate *what* the individual communicated about or read. Moreover, the purpose of the government surveillance in *Smith* with respect to telephone numbers was simply to determine *who* Smith called. The purpose of the government surveillance here with respect to Web site IP addresses was to determine *what* Alba read on the Web--in other words--the content.

that information to engage in more expansive surveillance. The government submitted the Coffey Affidavit to support its application.

That the government's surveillance in this case obtained content information is not surprising because Web site IP addresses often reveal content information. On their face, Web site IP addresses look like a meaningless collection of numbers (i.e. 65.57.252.248 or 207.97.211.98). But these Web site IP addresses, like many Web site IP addresses, correspond to specific Web sites (i.e. National Right to Life or BreastCancer.org).⁴ The fact that the government may not know which specific pages within a Web site an individual viewed does not mean that no content information has been revealed. As the panel notes, knowing an individual visited the New York Times Web site is not as revealing as knowing the specific page viewed because that particular Web site consists of many pages on a variety of topics. Slip op. at 8084 n.6. But few Web sites are as large and all encompassing as the New York Times site. Many have specific missions and few pages (i.e. www.StudentsAgainstSweatshops.org or www.StopTeenDrugAddiction.com). Knowing the Web site viewed is functionally equivalent to knowing the subject of the content viewed.

⁴ As the panel acknowledges, many IP addresses are only associated with a single or a handful of sites. Slip op. at 8083. *See also* Ben Edelman, *Web Sites Sharing IP Addresses: Prevalence and Significance*, <http://cyber.law.harvard.edu/people/edelman/ip-sharing/>.

Web site IP addresses are analogous to Dewey Decimal numbers. Like many Web sites, every book in a library is assigned a unique identifier, such as “616.462 JAR” or “342.084 LEE.” Like many Web site IP addresses, these seemingly meaningless numbers correspond to specific content, in this case J. M. Dixon, *ABCs of Breast Diseases* (2000), and Ellie Lee, *Abortion Law and Politics Today* (1998). The fact that the government does not know which specific pages of *ABCs of Breast Diseases* an individual read does not give the government the right to obtain that person’s reading records without a warrant.

In the context of book records, courts have held that because of the nexus of First and Fourth Amendment interests at stake, the government must show a “compelling need” to execute a subpoena for bookstore records. *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, 26 Media L. Rep. (BNA) 1599, 1601 (D.D.C. 1998) (holding that the government must show a compelling need to access book purchase records, and finding that “[m]any customers . . . informed Kramerbooks personnel that they will no longer shop at the bookstore because they believed Kramerbooks to have turned documents over. . . that reveal a patron’s choice of books”); *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1053 (Colo. 2002) (invalidating a search warrant seeking records of a particular

customer's past purchases, and noting that "the First Amendment embraces the individual's right to purchase and read whatever books she wishes to, without fear that the government will take steps to discover which books she buys, reads, or intends to read."). This same principle should be applied to the Web sites an individual reads. This Court should hold that the government cannot intercept or monitor Web site IP addresses without a warrant.

Third, and finally, the panel disregards the societal expectation that an individual's Web usage is private. The Web is the most expansive collection of human knowledge ever compiled. *See Reno v. ACLU*, 521 U.S. at 870. The barriers to use are low, and individuals read the Web on a wide range of topics, many highly personal. According to the Pew Research Center, 79 percent of American Internet users (111 million people) read the Web to find health and medical information; 30 percent (42.3 million people) look for religious or spiritual information; 28 (39.48 million people) percent look for information about someone they know or might meet; and 11 percent (15.51 million people) go to online dating Web sites. Pew Internet & American Life Tracking Surveys (March 2000 – Dec. 2006), *Internet Activities*, available at www.pewinternet.org/trends/Internet_Activities_1.11.07.htm. The Internet is a freewheeling marketplace of ideas in no small part because

of the societal expectation that individuals can read the Web without risk of observation or fear of social stigma, an expectation reinforced by the fact that individuals frequently read the Web from the seclusion of their own homes.⁵ Thus, this case stands in marked contrast to *Smith*, where the Supreme Court concluded that Smith's conduct was not calculated to preserve privacy. Slip op. at 8083 (quoting *Smith*, 442 U.S. at 743).

Given the foregoing, this Court should grant rehearing or rehearing en banc and hold that the government needs a warrant to intercept or monitor the IP addresses of the Web sites a user reads because Web IP addresses reveal content.⁶

⁵ That people expect their online reading to remain private was recently demonstrated by the public uproar when AOL inadvertently publicly released the search histories of over 650,000 individuals. See Declan McCullagh, "AOL's Disturbing Glimpse Into Users' Lives," CNET News.com, Aug. 7, 2006, available at http://news.com.com/AOL+offers+glimpse+into+users+lives/2100-1030_3-6103098.html. A similar outcry occurred when the government subpoenaed Web usage records from Google. Vanessa Ho et al, *Web-File Request Raises Privacy Fears*, Seattle Post-Intelligencer, June 2, 2006.

⁶ Although not the subject of this brief, email addresses, like IP addresses, can reveal the content of a communication. For example, email addresses may directly communicate the content of a message, e.g., BushVoter@well.com or kerryfan@well.com, while the email addresses from which email newsletters are sent may directly identify the name or topic of the newsletter, e.g., Free_Israel_of_Palestine@yahoogroup.com or Palestine_Info_Hamas@yahoogroups.com. See Brief of Amicus Curiae Electronic Frontier Foundation, et al., in Support of Plaintiffs, Doe v.

II. The Panel's Sweeping Dicta Eviscerates Fourth Amendment Protection for All Internet Communications and Conflicts With Supreme Court Precedent.

The panel's opinion suffers from an additional flaw. The reasoning on which its conclusion is based is so sweeping that it would eliminate Fourth Amendment protection for all Internet communications, not just for viewed Web site IP addresses. The panel explained its rationale as follows:

Smith based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment. Analogously, e-mail and Internet users have no expectation of privacy in . . . the IP addresses of the websites they visit because they should know that . . . these IP addresses are accessed through the equipment of their Internet service provider and other third parties.

Slip op. at 8083.

This interpretation of *Smith* is too broad. By its nature, the Internet involves transmitting information "through the equipment of their Internet service provider and other third parties." Slip op. at 8083. Every single communication conveyed via the Internet travels through the equipment of a third party. This includes the content of emails as well as the To/From and Subject lines of emails. So, too, does it include the content of specific Web

Ashcroft, 334 F.Supp.2d 471 (S.D.N.Y. 2004), vacated by *Doe v. Gonzales*, 449 F.3d 415 (2nd Cir. 2006), at 12-16, available at 2004 WL 2544692.

pages as well as the IP addresses of Web sites. Every instant message, Voice over IP telephone call, and file transfer is covered.

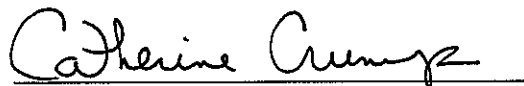
The panel's reasoning is inconsistent with the line the Supreme Court drew in *Katz* and *Smith*. As noted above, those cases hold that individuals have a reasonable expectation of privacy in their communications if content information is revealed. *Katz*, 389 U.S. at 352; *Smith*, 442 U.S. at 741. The panel's expansive reasoning fails to recognize the line the Court set out between content and non-content information. At minimum, the opinion should be amended to clarify that the mere fact that communications are accessed and transmitted over the network of third parties or with the aid of an Internet service provider does not eliminate a reasonable expectation of privacy in them, and that where the government intercepts or monitors content, it needs a warrant.

CONCLUSION

For the foregoing reasons, the petition should be granted.

Respectfully submitted,

Dated: August 28, 2007



Catherine Crump

Aden J. Fine

American Civil Liberties Union Foundation

125 Broad Street, 17th Floor

New York, NY 10004-2400

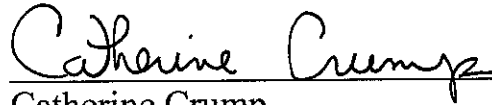
(212) 519-7806

Attorneys for Amici Curiae

CERTIFICATE OF COMPLIANCE

I certify that this amicus brief is not subject to the type-volume limitations because it is an amicus brief of no more than 15 pages and complies with Fed. R. App. P. 32(a)(1)-(5).

Dated: Aug. 28, 2007



Catherine Crump
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, NY 10004-2400
(212) 549-7806

PROOF OF SERVICE

I, the undersigned, hereby declare under penalty of perjury that I am a citizen of the United States and over the age of eighteen years and not a party to this action. My business address is American Civil Liberties Union Foundation, 125 Broad Street, 17th Floor, New York, NY 10004-2400. On this date, I served by Federal Express the **AMICUS BRIEF IN SUPPORT OF APPELLANT ALBA'S PETITION FOR REHEARING AND SUGGESTION FOR REHEARING EN BANC** on:

Michael L. Crowley
550 West "C" Street, Suite 1960
San Diego, CA 92101
Attorney for Mr. Alba

Todd Robinson
Assistant U.S. Attorney
880 Front Street, Room 6293
San Diego, CA 92101-8800

Benjamin Coleman
433 "G" St., Ste. 202
San Diego, CA 92101
Attorney for Mr. Forrester

Dated: Aug. 28, 2007


Christina Juhász-Wood