NOTES

PRIVACY, FREE SPEECH, AND THE PATRIOT ACT: FIRST AND FOURTH AMENDMENT LIMITS ON NATIONAL SECURITY LETTERS

PATRICK P. GARLINGER*

Congress's passage of the Patriot Act after 9/11 expanded the Federal Bureau of Investigation's (FBI) information-gathering authority to issue national security letters (NSL). Without any judicial review, the FBI issues NSLs to telecommunications providers to obtain customer subscriber information, including sources of payment, records of Internet activity, addressees and subject lines of emails, websites visited, and search queries. Because a subscriber has voluntarily given the data to a third party, the NSL is not considered a "search" for Fourth Amendment purposes, under the so-called "third-party doctrine." To overcome this constitutional shortcoming, commentators have argued that the chilling effect NSLs have on the exercise of free speech makes such investigations suspect under the First Amendment.

Despite the appeal of the First Amendment argument, this Note argues that a subscriber's free speech claim against an NSL faces more significant doctrinal hurdles than scholars have recognized: The First Amendment does not directly protect privacy, making a chilling effect claim hard to sustain. Furthermore, the standard of review in First Amendment cases may be too deferential to the government because the Patriot Act does not directly target speech, only data related to communicative activity. Instead, this Note proposes statutory reform for more enhanced judicial review and considers how the First Amendment could be used, not as an independent challenge, but rather as a basis for modifying the third-party doctrine. The Note concludes that the concern for chilling free speech is valid, and although First Amendment doctrine may not provide the means to defeat an NSL, concern for free speech interests could provide courts with a rationale for finding a reasonable expectation of privacy in Internet data, thus strengthening our currently impoverished Fourth Amendment safeguards.

 J.D., 2009, New York University School of Law; B.A., 1994, Washington University in St. Louis. I wish to thank, first and foremost, Geoffrey Stone for providing substantial feedback and insightful suggestions for improving the piece. I am indebted to Stephen Schulhofer for inspiring me to write a seminar paper on the topic and later encouraging its evolution into a student Note. I am thankful for helpful advice about writing and legal scholarship from Rachel Barkow, Barry Friedman, Cristina Rodríguez, Samuel Issacharoff and participants in the Furman Academic Scholars program. I am immensely grateful to Jeremy Weinberg, the editor of this Note, as well as to Tabatha Abu El-Haj, Kevin Arlyck, Brian Burgess, Rebecca Stone, Matt Lawrence, Aaron Clark-Rizzio, Julia Sheketoff, Carmen Iguina, and Nate Wessler for reading and providing constructive remarks on earlier drafts. Finally, I thank Drew Johnson-Skinner, Rachel Goodman, Kristen Richer, Melissa Krenzel Lang, and the staff editors of the *New York University Law Review* for their considerable editorial assistance as they shepherded the Note to publication.

INTRODUCTION

In 2007, in *Doe v. Gonzales*,[1] a federal district court relied on the First Amendment to invalidate key provisions of the USA PATRIOT Act (Patriot Act or Act),[2] which authorizes the Federal Bureau of Investigation (FBI) to send a National Security Letter (NSL) to any Internet service provider (ISP). The NSL, a form of administrative subpoena,[3] requests subscribers' information, such as Internet protocol (IP) addresses, lists of the websites the subscriber has visited, including Google searches, and records of the subscriber's email communications with correspondents' names and subject lines.[4] The FBI can issue an NSL without any judicial review.[5]

In *Doe*, the FBI had issued an NSL to an unnamed ISP, known as John Doe, with a gag order prohibiting the ISP from discussing the NSL with anyone except its counsel.[6] The district court invalidated that provision, holding that it infringed on the ISP's freedom of speech by preventing it from speaking publicly about the NSL.[7] Nevertheless, the district court did not directly invalidate the provisions relating to the production of information and did not base its analysis on the privacy or speech interests of the individuals whose information was requested.[8] *Doe* thus left open a fundamental question: Could an individual subscriber prevent the disclosure of his information by relying on either the First or the Fourth Amendment?

---

1 500 F. Supp. 2d 379 (S.D.N.Y. 2007).

2 Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 505, 115 Stat. 272, 365–66 (codified as amended at 18 U.S.C. § 2709(b) (2006)).

3 For an overview of the distinctions between ordinary subpoenas and NSLs, see STEPHEN J. SCHULHOFER, RETHINKING THE PATRIOT ACT: KEEPING AMERICA SAFE AND FREE 56, 58–59 (2005).

4 *See infra* notes 54–55 and accompanying text.

5 *See infra* note 59 and accompanying text.

6 Doe v. Ashcroft (*Doe I*), 334 F. Supp. 2d 471, 478–79 (S.D.N.Y. 2004); *see also* 18 U.S.C. § 2709(c) (2000) (providing statutory prohibition on disclosure of NSLs to "any person" other than recipient electronic communication service provider and its counsel). Later amendments allow a recipient, who will often have little incentive to challenge an NSL, to seek to quash the request through a deferential form of judicial review in district court. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 115(a), 120 Stat. 192, 211–13 (codified as amended at 18 U.S.C. § 3511(a) (2006)).

7 *Doe I*, 334 F. Supp. 2d at 507–08, 514. The Internet subscribers' free speech claim against the document production provisions of the statute authorizing NSLs was dropped before the 2007 ruling on the constitutionality of the nondisclosure provision. See Part I.C for a full discussion.

8 The district court invalidated both the production and nondisclosure provisions, but only because it found the offending nondisclosure provision to be unseverable from the rest of the statutory scheme. *See infra* notes 102–05 and accompanying text.

In each year since the Act's passage, the FBI has requested that telephone companies and electronic communication service providers (ECSPs) proffer information concerning anywhere from 16,000 to 50,000 people.[9] Critics have lambasted the Patriot Act as overreaching to protect national security at the expense of civil liberties.[10] Because the Fourth Amendment protects a person's freedom from unreasonable searches and seizures and provides the primary defense against government invasions of privacy, one might presume that the Fourth Amendment would limit the government's ability to acquire such information without prior judicial review.[11] However, the Fourth Amendment currently does not extend to information voluntarily given to third parties such as ISPs.[12] The government, therefore, can access private information held by ISPs with little oversight or accountability.

Does the First Amendment provide an alternative means for individual subscribers to challenge this access? In the absence of a Fourth Amendment check on government surveillance and information gathering from third parties,[13] some critics appeal to the First Amendment[14] as a means of challenging such practices. Since data from

---

[9] *See infra* note 64 and accompanying text.

[10] *See, e.g.*, Laurie Thomas Lee, *The USA PATRIOT Act and Telecommunications: Privacy Under Attack*, 29 RUTGERS COMPUTER & TECH. L.J. 371, 371 (2003) ("By enhancing the government's ability to conduct surveillance, . . . this far-reaching legislation severely diminishes critical privacy protections to an 'unprecedented degree.'"); Patricia Mell, *Big Brother at the Door: Balancing National Security with Privacy Under the USA PATRIOT Act*, 80 DENV. U. L. REV. 375, 379 (2002) ("The PATRIOT Act attacks the balance between the government and the individual by a systematic circumvention of established doctrine and procedures guarding against unreasonable governmental intrusion."); Christopher P. Raab, *Fighting Terrorism in an Electronic Age: Does the Patriot Act Unduly Compromise Our Civil Liberties?*, 2006 DUKE L. & TECH. REV. ¶¶ 3, 11–17, 26–33 (discussing provisions of Patriot Act and concluding they infringe civil liberties); Andrew E. Nieland, Note, *National Security Letters and the Amended Patriot Act*, 92 CORNELL L. REV. 1201, 1227–31 (2007) (discussing how Patriot Act changes to NSL statute and Patriot Act reauthorization raise "civil libertarian" concerns and bespeak trend toward broad compulsory subpoena power for FBI). For an opposing view, that the Act made minor modifications to the NSL statute and included more safeguards, see Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 608 (2003) ("[T]he Patriot Act generally offers a balanced approach that in some ways protects civil liberties more than the laws it replaced.").

[11] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

[12] For discussion of the third-party doctrine, see *infra* notes 43–49 and accompanying text.

[13] "Surveillance" refers to the direct monitoring of individuals or groups and their activities; "information gathering" refers to the collection of already existing information from third parties. I focus principally on the latter.

[14] U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech . . . .").

Internet and telephone companies is derived from speech and communication, they assert, the government's action implicates the First Amendment's protection of freedom of speech and association.[15] Despite the considerable appeal of the free speech argument, this Note argues that the First Amendment is ultimately insufficient to protect the public from the FBI's use of NSLs to gather information.[16] While critics have advanced persuasive arguments as to why First Amendment values are implicated by NSLs,[17] few have acknowledged the doctrine's limited ability to protect individuals' private information.[18] This Note aims to demonstrate why reliance on the First Amendment is unlikely to solve the problem of overreaching government information gathering by arguing that a litigant must meet too high a burden to prove a link between the compelled disclosure of Internet activity data and a chilling effect. Further, when faced with the task of balancing national security and individual privacy, a court may be more likely to favor the government's interest.[19] Finally, relying on the First Amendment in this context might have the perverse effect of weakening the doctrine, as it risks importing more deferential Fourth Amendment standards into First Amendment jurisprudence.

Instead, I argue that two changes might enable better privacy protection: statutory reform providing for more robust judicial review, or, as this Note favors, revision of the Fourth Amendment third-party doctrine. Although First Amendment doctrine may not provide a litigant with adequate means to challenge an NSL, the impact of infor-

---

[15] *See* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 117–23 (2007) (arguing that "current criminal procedure rules under-protect First Amendment activities, leaving them exposed to intrusive government information gathering"); *see also* Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance, and the Privacy of Groups*, 46 ARIZ. L. REV. 621, 626–27 (2004) (advocating freedom of association as protection against surveillance); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 749 (2008) (same).

[16] Although it principally discusses the NSL provisions, this Note's conclusions extend beyond them to other forms of government information gathering and surveillance.

[17] *See, e.g.*, Solove, *supra* note 15, at 167–68 (proposing First Amendment challenge to NSLs).

[18] *See, e.g.*, Matthew Lynch, *Closing the Orwellian Loophole: The Present Constitutionality of Big Brother and the Potential for a First Amendment Cure*, 5 FIRST AMENDMENT L. REV. 234, 266–69 (2007) (highlighting difficulty of demonstrating standing in First Amendment cases where government "merely" surveils and does not directly criminalize speech or association); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 428 (2008) (noting limitations of First Amendment doctrine due to focus on speech and writing).

[19] *Cf.* GEOFFREY R. STONE, PERILOUS TIMES: FREE SPEECH IN WARTIME FROM THE SEDITION ACT OF 1798 TO THE WAR ON TERRORISM 547 (2004) (noting "a repeated *pattern* of excessive restriction of civil liberties in wartime").

mation gathering on free speech interests, coupled with the Fourth Amendment's traditional concern for First Amendment values, could provide a basis for establishing a reasonable expectation of privacy in Internet data.[20] Courts could modify the third-party doctrine by requiring that the government satisfy a heightened standard of proof when attempting to access electronic communications information.

This Note unfolds in three parts. Part I discusses Congress's expansion of NSL authority under the Patriot Act and the limited protection that the Fourth Amendment currently provides against government issuance of NSLs. It also details a recent series of cases that invalidated several NSL provisions under the First Amendment. Part II demonstrates that the First Amendment, too, provides only limited protection for the targeted Internet data and then analyzes the hurdles that subscribers may face in challenging an NSL. In particular, it focuses on (1) differences in how the First and Fourth Amendment treat privacy, and (2) how courts might balance national security and speech interests. In light of that analysis, Part III reviews proposed solutions that address privacy concerns in government information gathering in general and the Patriot Act in particular. It first looks to amending the Act to include statutory judicial review provisions that can help ensure that the FBI properly uses NSLs; it then offers an alternative proposal: to revise the third-party doctrine to expand Fourth Amendment protection in light of First Amendment concerns.

I
The Constitutionality of National Security Letters

This Part introduces the NSL provisions of the Patriot Act and the current constitutional challenges to them. Part I.A provides an overview of the original NSL provisions and the eventual expansion of the FBI's authority to issue NSLs under the Patriot Act. Part I.B explains the danger to privacy that NSLs pose and why, despite that danger, NSLs are constitutional under the Fourth Amendment's third-party doctrine. Part I.C examines a recent constitutional challenge to the FBI's NSL authority. There, the court found that the Fourth Amendment did not protect the information sought but held that certain NSL provisions violated the First Amendment, suggesting an alternative constitutional protection against government information gathering.

---

[20] *See infra* Part III.B.

A. The FBI's Authority to Issue NSLs

Authority to issue NSLs was originally granted by the Electronic Communications Privacy Act (ECPA), a complex statutory scheme that outlines procedures the government must follow to obtain information from telephone companies and ECSPs during an investigation.[21] Congress enacted the ECPA in 1986, aiming to balance users' privacy interests and the federal government's legitimate law enforcement needs.[22] On the law enforcement side, the ECPA provides the FBI with a device, the NSL, that allows it to gather information rapidly for anti-terrorism and counterintelligence purposes. Because the ECPA aims to safeguard national security interests in advance of conflict, efficiency is crucial.[23] This goal differs from that of ordinary criminal prosecution, which focuses on offenses already committed and therefore demands less expeditious action. On the privacy side, the original NSL provision of the ECPA[24] imposed a number of limits on the reach of the NSL, including scope, nexus, and certification requirements. It defined the scope of the NSL to reach only user records "relevant to an authorized foreign counter-intelligence investigation."[25] The Agency also had to allege "specific and articulable facts" showing a nexus between the information sought and "a foreign power or an agent of a foreign power."[26] Further, the request had to be certified by the Director or an Assistant Deputy Director of the FBI.[27] If these three conditions were met, the ECPA allowed NSLs to obtain subscriber information, toll billing records, and "electronic communication transactional records."[28] It did not, however, provide

---

[21] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). The first instantiation of the NSL appeared in the 1978 Right to Financial Privacy Act (RFPA), but compliance was not mandatory. See Nieland, *supra* note 10, at 1207–09, for a concise history of the NSL.

[22] Nieland, *supra* note 10, at 1209; Zachary D. Shankman, Note, *Devising a Constitutional National Security Letter Process in Light of* Doe v. Ashcroft, 94 GEO. L.J. 247, 250 (2005).

[23] *See* Shankman, *supra* note 22, at 256–57 (discussing argument that efficient subpoena process is necessary in counterterrorism efforts).

[24] Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1867 (1986) (codified as amended at 18 U.S.C. § 2709 (2006)). Section 2709 was enacted as part of Title II of the ECPA—titled the Stored Communications Act—which covers email stored on an ISP's servers.

[25] 18 U.S.C. § 2709 (1988).

[26] *Id.* In 1993, Congress broadened the scope of § 2709 to permit the issuance of an NSL to obtain information from a subscriber who had communicated with a foreign agent regarding terrorist or intelligence activities. FBI Access to Telephone Subscriber Information Act, Pub. L. No. 103-142, § 1, 107 Stat. 1491, 1491–92 (1993) (codified as amended at 18 U.S.C. § 2709 (1994)); *see also* Shankman, *supra* note 22, at 251.

[27] 18 U.S.C. § 2709(b) (1988).

[28] This phrase is left undefined in the statute. 18 U.S.C. § 2709(a) (1988); *see infra* text accompanying notes 50–53 (discussing rise in use of ISPs and resulting ambiguity as to

for judicial review.[29] In sum, if the Director or Assistant Deputy Director of the FBI certified that he had specific information linking an individual to a terrorism investigation, the agency could obtain that user's records.

Section 505 of the Patriot Act expanded the FBI's NSL authority in a number of ways.[30] It broadened the permissive scope of such investigations from "authorized foreign counterintelligence investigation[s]" to include those designed "to protect against international terrorism or clandestine intelligence activities."[31] It relaxed the nexus standards, replacing the "specific and articulable facts" requirement with a vague "relevance" standard,[32] and relaxed the certification requirement by allowing designated agents in field offices to issue NSLs.[33] Finally, the Act expanded the categories of information that an NSL provides authority to obtain.[34] Basic subscriber information—formerly limited to financial data, telephone records, and consumer credit reports—came to include information regarding the types of services used, any "temporarily assigned network addresses," and sources of payment.[35] In short, the Patriot Act allowed field officers to certify, without providing any specific facts, that an individual's data is "relevant" to an investigation designed to protect against terrorist activities, and it authorized the FBI to issue an NSL on that basis alone.

B. The Limited Protection of the Fourth Amendment

Despite the fact that NSLs compel disclosure of individuals' private data, the issuance of an NSL does not violate any privacy interest

---

whether ISP envelope information is within scope of "electronic communication transaction record").

[29] *See infra* notes 59–61 and accompanying text. The statute also did not provide any enforcement mechanism for compelling production or enforcing the nondisclosure requirement. *See* Nieland, *supra* note 10, at 1210 (discussing legislative history of ECPA). It appears that the drafters assumed the NSL would be used infrequently. *Id.* ("NSL authority was initially intended as a limited alternative to . . . the compulsory process of a subpoena.").

[30] USA PATRIOT Act, Pub. L. No. 107-56, § 505, 115 Stat. 272, 365 (2001) (codified as amended at 18 U.S.C. § 2709(b) (2006)).

[31] USA PATRIOT Act § 505(a)(2)(B); 18 U.S.C. § 2709(b) (1988).

[32] *Id.*

[33] *Id.*

[34] SCHULHOFER, *supra* note 3, at 62. For example, financial institutions now include pawn shops and travel agencies. Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83, 87 (2006), http://www.harvardlawreview.org/forum/issues/119/dec05/zittrainfor05.pdf.

[35] 18 U.S.C. § 2703(c)(2)(D)–(F) (Supp. I 2001–2002). Acquiring access to contents of electronic communications still requires a warrant if they have been on an ISP's servers for 180 days or less. 18 U.S.C. § 2703(a).

an individual can currently claim under the Fourth Amendment. In fact, the ECPA was passed in response to developments in Fourth Amendment jurisprudence that diminished any constitutional protection for users' information.[36] This section situates NSLs within Fourth Amendment doctrine, explaining the difficulty of a Fourth Amendment challenge to the statute and the dangers that NSLs pose to privacy interests. This background helps to contextualize the appeal of using the First Amendment as an alternative ground for challenging NSLs.[37]

The Fourth Amendment explicitly protects the people from unreasonable government searches.[38] Justice Brandeis eloquently described it as "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[39] In *Katz v. United States*,[40] the seminal Fourth Amendment case, the Supreme Court established that the Fourth Amendment applies to areas in which an individual maintains a "reasonable expectation of privacy."[41] Activities undertaken within that realm of privacy are presumptively shielded from government scrutiny; to pursue an investigative search within that realm, law enforcement officials generally must obtain a warrant issued on probable cause that evidence of a crime will be found.[42] To ensure that innocent citizens are not subjected to intrusion, a detached and neutral magistrate must issue the warrant prior to the search.[43]

However, an individual has no Fourth Amendment claim when the government acquires information that has been given voluntarily to a third party. Where there is no expectation of privacy, the govern-

---

[36] *See infra* notes 43–48 and accompanying text.

[37] *See infra* Part I.C.

[38] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

[39] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[40] 389 U.S. 347, 353 (1967) (holding use of spike-mike to listen to petitioner's conversation in public telephone booth without warrant violated Fourth Amendment).

[41] *Id.* at 360 (Harlan, J., concurring).

[42] U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); *see* Coolidge v. New Hampshire, 403 U.S. 443, 455 (1971) (noting that exceptions to requiring warrant prior to search are "jealously and carefully drawn" and exigency must be established (quoting Jones v. United States, 357 U.S. 493, 499 (1958))); *Katz*, 389 U.S. at 357 ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." (citation omitted)).

[43] *See, e.g.*, *Coolidge*, 403 U.S. at 450 (holding that State Attorney General, as prosecutor, could not issue warrant).

ment's activities are not deemed to be a search for the purposes of the Fourth Amendment.[44] Voluntary disclosure to a third party, like giving financial information to a bank, eliminates any expectation of privacy in that information, and therefore no warrant is required.[45] Similarly, the act of dialing phone numbers is a voluntary disclosure of that data to a telephone company, thus making it permissible for the government to install a pen register, which records those numbers, without a warrant.[46] The theory animating the third party doctrine is that, by providing information to a third party, an individual assumes the risk that the third party will disclose that information to law enforcement authorities.[47] It was because of the gap in Fourth Amendment protection created by the third-party doctrine that Congress passed the ECPA, which provided some, albeit limited, statutory safeguards for user information.[48]

Since the passage of the ECPA, the development of the Internet and the proliferation of its uses have exacerbated the potential for privacy violations by expanding both the type and the amount of information accessible to the government without a warrant. First, courts have extended the third-party doctrine to cover Internet activity data. By analogizing the transmission of IP addresses to the dialing of phone numbers and by emphasizing that a subscriber has entered into a voluntary business relationship with an ISP, courts find Internet data to have been voluntarily disclosed to a third party.[49]

---

[44] *See, e.g.*, California v. Greenwood, 486 U.S. 35, 40–41 (1988) (finding no reasonable expectation of privacy in garbage bags left for collection and thus declining to require warrant to search their contents).

[45] United States v. Miller, 425 U.S. 435, 442 (1976) (upholding subpoena based on absence of "legitimate 'expectation of privacy'" because information was "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business").

[46] Smith v. Maryland, 442 U.S. 735, 743 (1979) (upholding warrantless use of pen register on ground that "it is too much to believe that telephone subscribers . . . harbor any general expectation that the numbers they dial will remain secret").

[47] *Id.* at 744 ("Because the depositor [in *Miller*] 'assumed the risk' of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private."); *see also* Reporters Comm. for Freedom of the Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1050 n.67 (D.C. Cir. 1978) (asserting that journalists assume risk of disclosure of confidential relationship with sources contacted through third party).

[48] Doe v. Ashcroft (*Doe I*), 334 F. Supp. 2d 471, 481 (S.D.N.Y. 2004) (citing S. Rep. No. 99-541, at 3 (1986)).

[49] *See* Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (applying third-party doctrine to subscriber information for Internet bulletin board and asserting that "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator"); *see also* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212 (2004) (summarizing "reasons [that] make it difficult for robust Fourth Amendment protections to apply online"). See Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth*

The rationale used to justify these decisions is that, because an ISP has access to data about a subscriber's web activity for internal business purposes, the user has no reasonable expectation of privacy.[50] As a result, the government can obtain Internet transactional and user data without a warrant.

The second major cause of increased government access to private information is the amount of that information now available from third parties. We place considerably more information in the hands of third parties, particularly in ISPs,[51] than we have in the past.[52] Much of our communication, in the form of emails, text messages, and blogs, now passes through ISPs. Similarly, we increasingly conduct many of our financial transactions online (e.g., purchases, banking).[53] Since Congress has never clearly defined "electronic communication transaction record," an NSL could obtain email "envelope information," including IP addresses, the names of senders and recipients, subject lines, and dates, all of which are often recorded by an ISP.[54] NSLs may also reach uniform resource locators (URLs), thus allowing the FBI to track an Internet user's reading habits.[55] As a result, the law as currently understood allows an NSL to seek information that falls into

---

Amendment Protection, 2007 UCLA J.L. & TECH. 2, ¶ 6, http://www.lawtechjournal.com/articles/2007/02_070426_lawless.pdf, for an argument that the application of the third-party doctrine to Internet search records undermines "the Fourth Amendment's core tenet of protecting expectations of privacy."

50 *See, e.g.*, United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at *3 (4th Cir. Aug. 3, 2000) (upholding subpoena because information obtained by government "had been available to MindSpring employees in the normal course of business").

51 In addition, the number of third parties that come within the category of ECSPs subject to an NSL has expanded dramatically as more entities provide Internet or web-based services. *See* Nieland, *supra* note 10, at 1214 (noting that, according to FBI, ECSP is any library, university, business, political organization, or charity that "enables users to send messages through a web site").

52 *See* Solove, *supra* note 15, at 113–14 (referring to "massive amount of data about our lives" now maintained by third parties).

53 *See* Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 213 (2006) (discussing expanded use of third parties for digital storage of private documents, financial records, and personal items).

54 *See* Zittrain, *supra* note 34, at 87 (arguing that ISPs may treat "envelope information" as falling within "electronic communication transactional records"); Nieland, *supra* note 10, at 1214 (citing Memorandum in Support of Plaintiffs' Motion for Summary Judgment, Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004) (No. 04 Civ. 2614), 2004 WL 2402699, for claim that, according to FBI, electronic communication transactional record (ECTR) includes all websites accessed and recipient and subject-matter lines of all emails).

55 Since the URL of a Google search results page includes the search terms, this information may be made available to the government. *See* Zittrain, *supra* note 34, at 87 ("'[E]nvelope information' . . . includes such things as . . . perhaps the contents of Google or other search engine queries made by a subscriber, since such queries are usually embedded in the URLs visited by that subscriber.").

three different categories: (a) subscriber information, such as sources of payment and activity logs, (b) "envelope information," such as addressees and dates of emails, and (c) electronic data that is essentially content, such as URLs and the search engine queries they may contain.[56]

The NSL provisions thus combine with the realities of Internet usage and the third-party doctrine to allow the government access to a vast amount of Internet data. An Internet user has no Fourth Amendment rights in such data because the user has "assumed the risk" of disclosure by sharing it with the ISP. The FBI, in turn, relies on its expanded, ill-defined authority under the Patriot Act to ask the ISP for all information "which [the recipient] consider[s] to be an electronic communication transaction record."[57] The open-ended nature of the request leaves ISPs unclear as to what the statute requires; many divulge more data than the statute permits, including the actual content of communications, in order to comply fully with their perception of the FBI's mandate.[58]

The third-party doctrine excuses the government from its usual Fourth Amendment obligation to seek judicial review in the form of a warrant before seizing information from an ISP; the NSL statute fails to provide any substitute mechanism for judicial review.[59] Indeed, as noted earlier, NSLs come with gag orders that prevent recipients from notifying or alerting anyone but counsel of the existence of an NSL request.[60] This lack of judicial oversight and the inability to disclose receipt of an NSL provide little guarantee that the FBI is in fact seeking information "relevant to an authorized investigation."[61]

---

[56] 18 U.S.C. § 2709(a)–(b) (2006); Doe v. Gonzales (*Doe III*), 500 F. Supp. 2d 379, 387 (S.D.N.Y. 2007) (reviewing § 2709 and discussing range of information reached by NSL), *aff'd in part, rev'd in part sub nom.* John Doe, Inc. v. Mukasey (*Doe IV*), 549 F.3d 861 (2d Cir. 2008). URLs and search queries may be seen as forms of content since they reflect, like communications, the individual's intellectual life and thoughts.

[57] Doe v. Ashcroft (*Doe I*), 334 F. Supp. 2d 471, 509–10 (S.D.N.Y. 2004) (emphasis omitted) (noting that "electronic communication transaction record" is undefined in statute and could reasonably be interpreted to "require, at minimum, disclosure of all e-mail header information, including subject lines"), *vacated sub nom.* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006).

[58] *See* Dan Eggen, *FBI Found To Misuse Security Letters*, WASH. POST, Mar. 14, 2008, at A03, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/03/13/AR2008031302277.html (referring to government report that found "FBI agents made improper requests, collected more data than they were allowed to, or did not have proper authorization to proceed with the case").

[59] Congress amended the statute in 2005 to provide a limited form of review. *See infra* note 90 and accompanying text.

[60] *See supra* note 6 and accompanying text.

[61] 18 U.S.C. § 2709(b)(1) (2006).

The absence of external review has real consequences.[62] After September 11, 2001, a dramatic increase in the issuance of NSLs occurred.[63] Until 2007, the FBI issued close to 50,000 NSL requests each year,[64] without an adequate mechanism for ensuring proper justification. An audit by the inspector general reveals that, between 2003 and 2005, the FBI frequently sought records without proper authorization[65] and that it underreported to Congress the number of NSLs requested by more than 4600.[66] Although a recent report suggests the FBI has improved how it handles NSL requests,[67] internal FBI guidelines alone are unlikely to diffuse concerns about abuse of investiga-

---

62 This is especially true since abuse of NSLs is not a federal crime, unlike illegal wiretapping. The incentive to adhere to the statute's requirements or internal FBI guidelines is therefore even lower. *See* Declan McCullagh, *Judge Deals Blow to Patriot Act*, CNET NEWS, Sept. 6, 2007, http://www.news.com/Judge-deals-blow-to-Patriot-Act/2100-1028_3-6206570.html.

63 Lara Jakes Jordan, *More FBI Privacy Violations Confirmed*, USA TODAY, Mar. 6, 2008, http://www.usatoday.com/news/washington/2008-03-05-3415742883_x.htm ("The number of national security letters issued by the FBI skyrocketed in the years after the Patriot Act became law in 2001 . . . .").

64 In 2005, the FBI issued approximately 19,000 NSLs containing 47,000 NSL requests (each NSL may contain multiple requests for information). Doe v. Gonzales (*Doe III*), 500 F. Supp. 2d 379, 390 (S.D.N.Y. 2007) (citing OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS 120 (2007) [hereinafter OIG REVIEW I]), *aff'd in part, rev'd in part sub nom.* John Doe, Inc. v. Mukasey (*Doe IV*), 549 F.3d 861 (2d Cir. 2008). In 2006, the FBI issued nearly 50,000 NSL requests. OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND NSL USAGE IN 2006, at 9 (2008) [hereinafter OIG REVIEW II]. Recent numbers indicate that in 2008, the FBI made 24,744 NSL requests (excluding requests for subscriber information only), seeking information pertaining to 7225 different United States persons. Letter from Ronald Weich, Assistant Attorney General, to Harry Reid, Majority Leader, U.S. Senate 4 (May 14, 2009), *available at* http://www.fas.org/irp/agency/doj/fisa/2008rept.pdf. In 2007, the FBI made 16,804 NSL requests (excluding requests for subscriber information only), pertaining to 4327 different United States persons. *Id.* at 5.

65 OIG REVIEW I, *supra* note 64, at xxxiii (reviewing sample of FBI files to find at least twenty-two percent contained "at least one [error]," thus suggesting a "significant number" of improper requests); *see also* Eric Lichtblau, *F.B.I. Made 'Blanket' Demands for Phone Records*, N.Y. TIMES, Mar. 13, 2008, at A22, *available at* http://www.nytimes.com/2008/03/13/washington/13fbi.htm (noting that FBI has acknowledged "the use of 'blanket' records demands to justify the improper collection of thousands of phone records"); OIG REVIEW II, *supra* note 64, at 6 (noting that inspector general audit revealed at least eleven blanket NSLs issued in 2006). A blanket NSL is used to collect information on large numbers of individuals without indicating why the information for each person is relevant to an investigation. *See* Lichtblau, *supra*.

66 OIG REVIEW I, *supra* note 64, at xvii; *see also* Jordan, *supra* note 63 ("The FBI acknowledged it improperly accessed Americans' telephone records, credit reports and Internet traffic in 2006, the fourth straight year of privacy abuses . . . .").

67 In his 2008 report, Glenn Fine, Inspector General for the Department of Justice, asserted that the FBI had made significant improvements in its handling of personal data but acknowledged that violations were still occurring. OIG REVIEW I, *supra* note 64, at 6, 8.

tory powers given the agency's history of past violations.[68] In fact, the agency has withdrawn its NSL requests in the few instances where the recipient has refused to comply, as if to acknowledge that it has overreached.[69] However, as evidenced by a dearth of legal challenges,[70] most subpoena recipients simply have no incentive to resist the request;[71] they readily comply and remain silent. In short, NSLs pose a significant threat to individual privacy, and neither the Fourth Amendment nor statutorily mandated judicial review ameliorate that threat. A recent set of cases challenging the NSL statute demonstrates the point.

C. The Constitutional Challenge to the NSL Provisions

In February 2004, an ISP, John Doe, Inc., claimed that the ECPA's document production provisions violated the Fourth and First Amendments and that the nondisclosure requirement violated the First Amendment.[72] In *Doe v. Ashcroft* (*Doe I*), the district court agreed, holding § 2709's document production provisions to be unconstitutional under the Fourth and the First Amendments; it also declared § 2709(c), the nondisclosure provision, unconstitutional under the First Amendment.[73]

---

[68] In 1976, a Senate committee issued a report that detailed the FBI's unauthorized use of surveillance techniques—wiretapping, reading mail, and unauthorized searches—to gather information on civil rights and political groups. See Solove, *supra* note 15, at 139–40, for a discussion of the report and other instances of the FBI's abuse of intelligence gathering techniques. *See also* Fisher, *supra* note 15, at 628–32 (surveying history of FBI's domestic intelligence gathering efforts).

[69] *See, e.g.*, *Doe III*, 500 F. Supp. 2d at 386 n.3 (noting that government had withdrawn request for information), *aff'd in part, rev'd in part sub nom.* John Doe, Inc. v. Mukasey (*Doe IV*), 549 F.3d 861 (2d Cir. 2008). The Internet Archive, a digital library in San Francisco, recently challenged an NSL, and the FBI withdrew it. *See* Ellen Nakashima, *FBI Backs Off from Secret Order for Data After Lawsuit*, WASH. POST, May 8, 2008, at D1. For a detailed overview, see Electronic Frontier Foundation, Internet Archive et al v. Mukasey et al, http://www.eff.org/cases/archive-v-mukasey (last visited Apr. 4, 2009).

[70] As discussed in Part I.C, *Doe v. Ashcroft* was the first challenge to the constitutionality of the NSL provisions. Hence, nearly two decades passed without judicial scrutiny of the authority granted to the FBI.

[71] This is commonly the case with subpoenas, since the privacy interests of the individual whose information is being revealed and the privacy interests of the recipient are unlikely to align; the recipient typically has little incentive to initiate any judicial review. See SCHULHOFER, *supra* note 3, at 56, for a discussion of this dilemma.

[72] Doe v. Ashcroft (*Doe I*), 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004), *vacated sub nom.* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006).

[73] *Id.* at 475, 524–26.

During the pendency of the appeal from that decision, Congress amended the Patriot Act.[74] The Second Circuit vacated the decision and remanded it to the district court for reconsideration in light of the amendments.[75] On remand, in *Doe III* the plaintiffs dropped the Fourth and First Amendment claims against the document production provisions, leaving only the First Amendment claim against the nondisclosure provision.[76] The *Doe III* court's ruling reiterated the unconstitutionality of the nondisclosure provision under the First Amendment; the Second Circuit affirmed this portion of the holding.[77]

The next section traces in further detail the evolution of these cases to demonstrate how the Fourth Amendment gave way to the First Amendment as the basis for invalidating the NSL statute.

1. First and Fourth Amendment Challenges in the District Court

At the time the original suit was filed in 2004, § 2709 did not permit judicial review of NSL requests.[78] *Doe I* held that the absence of review violated the Fourth Amendment.[79] It is important, however, to recognize the limited nature of the ISP's Fourth Amendment claim in this instance.

In *Doe I*, the plaintiff sought to vindicate *its own* Fourth Amendment rights, as an ISP, to resist production of subpoenaed documents under § 2709(a) and (b). It did not assert that the subscribers themselves had a privacy interest in that information; nor did it seek to revise the third-party doctrine. The Southern District of New York acknowledged that NSL recipients, like all subpoena recipients, are

---

[74] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, §§ 115, 116, 120 Stat. 192, 211–17 (2006) (codified at 18 U.S.C. §§ 2709(c), 3511 (2006)).

[75] 449 F.3d at 421. *Doe I* was consolidated with a district court case in Connecticut, *Doe v. Gonzales* (*Doe II*), in which the government was enjoined from enforcing § 2709(c), the nondisclosure provision, on the ground that it was not sufficiently narrowly tailored. 386 F. Supp. 2d 66 (D. Conn. 2005). When the Second Circuit vacated *Doe I* and remanded back to the Southern District of New York for reconsideration in light of the Reauthorization Act, it dismissed *Doe II* as moot because the government had permitted the plaintiff to identify itself as a recipient of an NSL. Doe v. Gonzales, 449 F.3d at 419–21. Although plaintiffs had also challenged the constitutionality of the production provisions, the district court in *Doe II* had granted the preliminary injunction on § 2709(c) alone. *Doe II*, 386 F. Supp. 2d at 83.

[76] Doe v. Gonzales (*Doe III*), 500 F. Supp. 2d 379 (S.D.N.Y. 2007), *aff'd in part, rev'd in part sub nom.* John Doe, Inc. v. Mukasey (*Doe IV*), 549 F.3d 861 (2d Cir. 2008).

[77] *Doe IV*, 549 F.3d at 864, 881.

[78] *Doe I*, 334 F. Supp. 2d at 506.

[79] *Id.* at 505.

entitled to some Fourth Amendment protection.[80] When a subpoena compels an individual or entity to produce information, there is still some intrusion on privacy, even if that intrusion does not rise to the level of a physical search. The constitutionality of the subpoena thus depends on the availability of some form of judicial review.[81] The court held that review may employ a relatively permissive "reasonableness" standard: If issuing the subpoena is within the agency's authority and the request for information is sufficiently definite, the subpoena must only be "reasonably relevant" to a legitimate inquiry.[82] Importantly, this standard only protects the NSL *recipient's* Fourth Amendment right against unreasonable production of information or documents. In the shadow of the third-party doctrine, subpoenas are not seen to implicate the Fourth Amendment privacy rights of the *individual subscribers* whose information is sought.[83]

In addition to its Fourth Amendment argument, Doe challenged the government's information gathering on two separate First Amendment grounds. First, Doe argued that the possibility of compelled disclosure would chill subscribers' exercise of their First Amendment rights to communicate and associate freely.[84] Second, Doe challenged the requirement under § 2709(c) that the ISP remain silent about the disclosure of information.[85]

In addressing the plaintiff's claim with regard to subscribers' speech interests, *Doe I* held that the possibility of compelled disclo-

---

[80] *Id.* at 495 ("The Fourth Amendment's protection against unreasonable searches applies to administrative subpoenas, even though issuing a subpoena does not involve a literal physical intrusion or search.").

[81] *Id.* ("[T]he constitutionality of the administrative subpoena is predicated on the availability of a neutral tribunal to determine . . . whether the subpoena actually complies with the Fourth Amendment's demands."); *see also* SCHULHOFER, *supra* note 3, at 56 (noting judicial oversight protects against unrestricted official searches).

[82] *Id.*

[83] *See* Solove, *supra* note 15, at 125; *see also* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1284 (2004) (contrasting requirements for subpoenas and warrants); *Doe I*, 334 F. Supp. 2d at 494 n.118 ("[T]he *Fourth Amendment* rights at issue here belong to the person or entity receiving the NSL, not to the person or entity to whom the subpoenaed records pertain." (emphasis added)).

[84] *See* U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech."). As Part II.B will discuss more extensively, the First Amendment protects the freedom of speech—the right to express one's thoughts without the government restricting or regulating one's message. Its core concern is ensuring freedom to engage in public debate, and it thus limits the government's ability to suppress particular viewpoints and to prevent free association with others as part of political debate. *See, e.g.*, Robert Post, *Reconciling Theory and Doctrine in First Amendment Jurisprudence*, *in* ETERNALLY VIGILANT: FREE SPEECH IN THE MODERN ERA 153, 166–68 (Lee C. Bollinger & Geoffrey R. Stone eds., 2002) (describing "participatory" theory that First Amendment "safeguard[s] . . . public discourse from regulations that are inconsistent with democratic legitimacy").

[85] *Doe I*, 334 F. Supp. 2d at 475.

sure of private information could potentially chill individual subscribers' First Amendment rights and thus deter individuals from communicating freely.[86] Simply put, if the government could access data about subscribers' activity and perhaps use it against subscribers in a criminal proceeding, users might refrain from emailing and blogging, among other online activities. The court also underscored the right to anonymous speech: "Every court that has addressed the issue has held that individual Internet subscribers have a right to engage in anonymous Internet speech, though anonymity may be trumped in a given case by other concerns."[87]

With regard to Doe's claim that the § 2709(c) gag requirements violated the First Amendment, the *Doe I* court agreed that the provision violated the ISP's free speech rights. By preventing the ISP from speaking publicly about the burden imposed by an NSL or the propriety of the government's information-gathering techniques,[88] the gag order "impose[s] a permanent bar on disclosure in every case, making no distinction among competing relative public policy values over time, and containing no provision for lifting that bar when the circumstances that justify it may no longer warrant categorical secrecy."[89] *Doe I* thus held that the document production provisions, § 2709(a) and (b), posed problems for subscribers and ISPs under both the Fourth and First Amendments and addressed the constitutional concerns of ISPs with respect to the § 2709(c) gag order provision.

While the appeal was pending, Congress amended the Act to provide a highly limited form of judicial review, codified in § 3511.[90] In light of this amendment, the Second Circuit vacated *Doe I*.[91] On remand, the plaintiffs chose not to renew their Fourth Amendment

---

[86] *Id.* at 506–07, 511 (holding that rights to anonymous speech and association may be infringed without defining full scope of those rights) (citing Talley v. California, 362 U.S. 60 (1960) (invalidating California law that prohibited anonymous handbill distribution) and NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958) (precluding disclosure of membership list due to potential chilling effect on right of association)).

[87] *Id*. at 508. Without First Amendment protection for anonymous speech, the FBI could use an NSL to obtain a political campaign's email lists or the identity of an anonymous blogger who speaks out against the government, which might chill the exercise of First Amendment rights. *Id.* at 509–10.

[88] *Id.* at 514.

[89] *Id.* at 519 (emphasis omitted).

[90] *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 115, 120 Stat. 211 (codified as amended at 18 U.S.C. § 3511 (2006)), *invalidated by* Doe v. Gonzales (*Doe III*), 500 F. Supp. 2d 379, 382 (S.D.N.Y. 2007). Congress's amendments to the Patriot Act were largely a response to *Doe I*. *See* H.R. REP. NO. 109-174, pt. 1, at 39–41 (2005).

[91] Doe v. Gonzales, 449 F.3d 415, 419 (2d Cir. 2006) ("[W]e remand this case so that the Southern District of New York . . . can address the First Amendment issues presented

argument against the document production provisions[92] because the availability of a judicial review mechanism to quash NSL requests meant that the ISP's Fourth Amendment rights were now protected, albeit by a very deferential standard.[93] The plaintiffs also chose not to renew their First Amendment challenge to the document production provisions. The resolution of the Fourth Amendment claim seems simply to have swallowed up the First Amendment claim on behalf of the subscribers. Thus, in *Doe III*, the district court mentioned only in passing the potential chilling effect on subscribers' speech.[94]

Doe did, however, renew the First Amendment claim against the nondisclosure provision, although Congress had also amended § 2709(c) to allow for a case-by-case evaluation of the need for nondisclosure if requested.[95] Despite this amendment, *Doe III* essentially reiterated the court's prior holding.[96] The nondisclosure provision, § 2709(c), still operated as a prior restraint[97] that prevented the ISP from publicly discussing the NSLs.[98] Nor was the new judicial review provision, § 3511(b), sufficient to evaluate the nondisclosure requirement.[99] Relying on *Freedman v. Maryland*,[100] which established that the First Amendment requires ex ante judicial review of speech

---

by the revised version of § 2709(c), and the Reauthorization Act's new procedures and standards for judicial review . . . .").

[92] *Doe III*, 500 F. Supp. 2d at 389 ("Plaintiffs do not renew their Fourth Amendment challenge.").

[93] Section 3511(b)(2), the new judicial review provision for nondisclosure orders, requires the FBI's certification of the need for nondisclosure to be considered "conclusive" unless "bad faith" can be established. 18 U.S.C. § 3511(b)(2) (2006).

[94] *Doe III*, 500 F. Supp. 2d at 395 (noting "the seriousness of the potential intrusion into the individual's personal affairs and the significant possibility of a chilling effect on speech and association").

[95] To require nondisclosure, the Director or his agent now had to certify that disclosure would result in danger to national security or to an individual, or interfere with an investigation or diplomatic relations. 18 U.S.C. § 2709(c)(1) (2006).

[96] *Doe III*, 500 F. Supp. 2d at 396–97 ("The Court's analysis begins by noting that for the same reasons articulated in *Doe I*, . . . the nondisclosure provision of the revised § 2709, like its predecessor, embodies both a prior restraint and a content-based restriction on speech.").

[97] A prior restraint violates the First Amendment by restricting expression before the speaker has made an attempt to speak, rather than by punishing the speaker *after* the expression. *See* Alexander v. United States, 509 U.S. 544, 550 (1993) (describing "prior restraint" as "*forbidding* certain communications . . . in advance of the time that such communications are to occur" (quoting MELVILLE B. NIMMER, NIMMER ON FREEDOM OF SPEECH § 4.03, at 4–14 (1984))).

[98] In *Doe II*, the plaintiff was a library, not an ISP, 386 F. Supp. 2d 66, 70 (D. Conn. 2005), and the 2005 amendments exempted libraries from the requirements of 18 U.S.C. § 2709(f). *See* 18 U.S.C. § 2709(f). Nevertheless, libraries are not exempt if they provide "electronic communication service[s]" and thus the same concerns with respect to Internet use still apply. *See id.*

[99] *Doe III*, 500 F. Supp. 2d at 395–96 ("[T]his Court finds that the standard of review the Reauthorization Act directs that the courts must apply when a nondisclosure order is

restrictions, the district court found § 3511(b) unconstitutional because it depended on the NSL recipient to initiate such review.[101] Because the court also held that it could not sever § 2709(c) from the rest of the statute,[102] the free speech violation invalidated § 2709 in its entirety.[103]

It is significant for our purposes that *Doe III* focused *exclusively* on the *ISP*'s free speech interests, setting aside any questions about the potential chilling effect on subscriber speech.[104] The district court invalidated the document production provisions only because the court refused to sever the nondisclosure provision from the rest of the statute.[105] Despite the fact that the court's refusal to sever § 2709(c) led to the invalidation of the document production provisions alongside the nondisclosure provision, the plaintiff's decision not to reassert the claim about the chilling effect on subscribers' speech on remand meant that the court never addressed the merits of that claim. The First Amendment was therefore only indirectly involved in the invalidation of the production provisions.

2. *The Second Circuit Upholds the Free Speech Claim Against Nondisclosure*

On appeal, the Second Circuit's decision in *Doe IV* reiterated the emphasis on the ISP's free speech interests and affirmed, with some modifications, the district court's analysis.[106] Focusing on the deficiencies of the nondisclosure requirement and judicial review procedures, the three-judge panel narrowly interpreted those provisions to limit their constitutional infirmities.[107] First, the court interpreted

---

challenged, offends the fundamental constitutional principles of checks and balances and separation of powers.").

100 380 U.S. 51 (1965).

101 *Doe III*, 500 F. Supp. 2d at 405–06 ("[T]he third *Freedman* procedural safeguard does apply to judicial review of the NSL statute. Accordingly, it is the government that must bear the burden of going to court to suppress the speech and that must bear the burden of proof once in court.").

102 The district court reiterated its analysis in *Doe I*, 334 F. Supp. 2d 471, 525–26 (S.D.N.Y. 2004), stating that Congress's intent was for § 2709(a)–(c) to work together to ensure that government information gathering operated in secrecy. *Doe III*, 500 F. Supp. 2d at 424–25.

103 *Doe III*, 500 F. Supp. 2d at 424–25.

104 Recall that the subscriber free speech claim in *Doe I* was predicated on the production provision, not the nondisclosure provision. Doe argued that subscribers' speech was chilled by the threat that the ISP would be forced to reveal its subscribers' information, not the fact that the ISP would be forced to remain silent about that revelation. *See supra* text accompanying note 84.

105 *Doe III*, 500 F. Supp. 2d at 425.

106 549 F.3d 861, 864 (2d Cir. 2008).

107 *Id.* at 875–76.

§ 2709(c) to mean that the government must certify that any harm from the disclosure of the NSL be "related to 'an authorized investigation.'"[108] It also read § 3511(b) to require that the government provide a "good reason" for compelling nondisclosure, presenting "some reasonable likelihood" that harm to the investigation would ensue.[109] Second, unlike the district court, which read *Freedman* to render § 3511(b) unconstitutional,[110] the Second Circuit circumvented the *Freedman* requirement of ex ante judicial review for speech restrictions. It engaged in a saving construction by introducing sua sponte a "reciprocal notice procedure" by which the government would inform the recipient that it has ten days to request judicial review.[111] These modifications permit the FBI, now subject to increased judicial review, to continue issuing NSL requests. Thus, the *Doe* decisions demonstrate that the First Amendment can provide a limited constitutional safeguard where the Fourth Amendment, due to the third-party doctrine, falters. The First Amendment analysis in the *Doe* cases, though, protects only the speech interests of the ISP.

II
The First Amendment as Safeguard Against Government Information Gathering

This Note has thus far shown that the third-party doctrine limits the Fourth Amendment's ability to restrict the government's information-gathering practices. The Patriot Act's minimal safeguards, although sufficient to survive Fourth Amendment review, are not particularly strong. Further, while the Second Circuit found the NSL's secrecy requirement to violate the First Amendment rights of the ISPs, it said nothing about those of the subscribers. The question remains, then: Does NSL information gathering implicate subscribers' First Amendment interests?

This Part considers the advantages and disadvantages of using the First Amendment to protect subscribers' speech and privacy interests. Part II.A highlights the limitations of the *Doe* decisions, arguing that the privacy and speech interests of the subscribers have been lost in

---

[108] *Id.* at 875 ("[The] potential reach of the nondisclosure requirement can be reined in if all the enumerated harms are keyed to the same standard that governs information sought by an NSL, i.e., 'relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.'" (citing 18 U.S.C. § 2709(b)(1)–(2))).

[109] *Id.* at 875–76 (noting that 18 U.S.C. § 3511(b), which permits a court to "set aside" or "modify" a nondisclosure requirement, is "silent as to the burden of proof").

[110] *Doe III*, 500 F. Supp. 2d at 424–25.

[111] *Doe IV*, 549 F.3d at 879–81 (justifying new procedure by relying on authority to modify statute where modification will avoid constitutional defect).

the legal analysis and that the amended judicial review provision still provides inadequate protection. Part II.B considers whether the First Amendment could provide *subscribers* with a basis for challenging government information-gathering practices like the NSL. It addresses the arguments made by critics who have advocated the use of the First Amendment as a safeguard against government surveillance and argues that litigants who attempt to challenge the NSL provisions using the First Amendment will be stymied principally by two factors: (1) the difficulty in determining which Internet data implicates First Amendment interests, and (2) the standard of review used in First Amendment balancing tests.

A. The Limits of Protecting ISP Free Speech Interests

Throughout the *Doe* litigation, the court focused on the ISP's speech concerns, rather than on those of the subscribers. What began as a series of First and Fourth Amendment challenges aimed at protecting the privacy interests of both the ISP and its subscribers evolved into a case about the ISP's free speech right to disclose its receipt of an NSL. Privacy concerns and the Fourth Amendment analysis fell by the wayside as the courts' opinions focused increasingly on the nondisclosure provision. Limited by the issues presented on appeal, the Second Circuit tailored the procedural safeguards and judicial review to protect some free speech values—the ISP's freedom to disclose that it had received an NSL—but not the Fourth Amendment privacy interests.

The free speech argument against the nondisclosure provision has salutary benefits, of course. Importantly, the standard of review under the First Amendment is more stringent than the Fourth Amendment standards for subpoenas. While the former requires narrow tailoring and a "good" justification for infringing on free speech by compelling nondisclosure, the latter requires only that the information sought be relevant to an investigation in order to justify an invasion of privacy.[112] As a result, the free speech interests of the ISPs are given greater weight than their Fourth Amendment privacy interests against producing information. The First Amendment requirement that judicial review be available to the recipient can force the government to justify the secrecy of the NSL,[113] and public knowledge of such a request may contribute to public discourse about the

---

[112] *Id.* at 875–76.

[113] The Second Circuit did not determine whether the FBI's voluntary acceptance of judicial review would be sufficient or whether Congress needed to amend the statutory provisions. *Id.* at 884.

propriety of government information-gathering practices.[114] Hence, robust protection of the ISP's free speech interests can, to an extent, deter the government from overreaching in its information gathering.

Nevertheless, the principal problem with NSLs is not the secrecy of the process but the compelled disclosure of private information; *Doe*'s focus on the nondisclosure provision protects subscribers' information only indirectly. The emphasis on judicial review is designed primarily to protect against harms stemming from forced nondisclosure of the subpoena, not those stemming from the production of the subscriber's information to the government. *Doe III* did not invalidate the judicial review provision for challenging the compelled production of information, § 3511(a).[115] That provision is presumably unaffected by the Second Circuit's reinterpretation of § 3511(b), and therefore the law does not require the government to inform the NSL recipient that it will seek judicial review of the production request if asked within ten days.[116] While the government might justify the need for the information as it attempts to demonstrate the requirement for nondisclosure, the subscriber still lacks the opportunity to seek judicial review of the subpoena itself. Further, the reciprocal notice procedure, which requires the government to inform the recipient ISP that it can ask the government to seek judicial review of the gag order, still relies on the *ISP's* incentive to voice its opposition.[117] In short, the ISP's free speech rights do little to prevent the disclosure of subscribers' information. The question thus becomes: In the absence of available Fourth Amendment protection, will subscribers be able to foreclose FBI access to that information through the First Amendment?

---

[114] Nondisclosure also prevents any "market" response by customers who might cancel service if they knew their ECSPs were cooperating with the government. As Zittrain notes, most ISP recipients choose to cooperate with the government and, in so doing, remain silent. *See* Zittrain, *supra* note 34, at 87–88.

[115] *Doe III*, 500 F. Supp. 2d at 425. Section 3511(a) allows the recipient ISP to quash the request only if the court finds that compliance would be "unreasonable, oppressive, or otherwise unlawful." 18 U.S.C. § 3511(a) (2006); *see also supra* note 90 and accompanying text.

[116] *See supra* Part I.C.2 (discussing Second Circuit's saving construction of § 3511(b) in John Doe, Inc. v. Mukasey (*Doe IV*), 549 F.3d 861, 879–81 (2d Cir. 2008), proposing that government provide notice of opportunity for judicial review).

[117] If the government meets its burden of showing the necessity of continued nondisclosure, the nondisclosure provision will take effect, and the ISP cannot challenge it again for a year. 18 U.S.C. § 3511(b)(3). Moreover, the compelling interest in national security might persuade a court that even after the information has served its purpose the nondisclosure order is still necessary. *See* United States v. Aguilar, 515 U.S. 593, 605–06 (1995) (upholding nondisclosure provision for expired wiretaps and crediting government's interest in secrecy over free speech interests in discussing defunct wiretaps).

B. The Difficulties of a First Amendment Challenge

Government surveillance and information gathering potentially implicate both the First and Fourth Amendments.[118] Such practices are, by their very nature, government infiltrations into private spheres of communication. As the Fourth Amendment was designed, in part, to safeguard First Amendment values, we are less concerned about the First Amendment when the Fourth Amendment warrant requirement is in effect.[119] But, as the NSL cases demonstrate, government surveillance and information gathering can chill free speech and association without triggering Fourth Amendment protections.[120]

In light of the limitations imposed by the Fourth Amendment's third-party doctrine, Daniel Solove makes a powerful argument for marshaling the First Amendment to advocate for additional procedural safeguards.[121] In many respects, the First Amendment functions as a strong bulwark against government intrusions. Under the highly speech-protective standard established by *Brandenburg v. Ohio*, speech that incites unlawful violence can be punished only if it expressly advocates unlawful activity and such activity is likely to be imminent.[122] Mere discussion of the merits of terrorist activity as a political strategy is thus protected by the First Amendment and

---

[118] *See* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 313 (1972) ("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."); *see also* GEOFFREY R. STONE, WAR AND LIBERTY: AN AMERICAN DILEMMA: 1790 TO THE PRESENT 142–43 (2007). The First and Fourth Amendments share a common origin and purpose: Historically they prevented the government from engaging in searches and seizures that affected freedom of the press. Solove, *supra* note 15, at 133–36. In *Marcus v. Search Warrant*, 367 U.S. 717 (1961), the Supreme Court acknowledged that limits on the government's authority to search and seize were necessary because of the government's desire to suppress publications that it deemed offensive. *Id*. at 724–29.

[119] Zurcher v. Stanford Daily, 436 U.S. 547, 564–65 (1978) (noting that Framers took into account need to protect against intrusion of press and asserting that "courts apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search"); *see also* Reporters Comm. for Freedom of the Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1054 (D.C. Cir. 1978) ("[O]ne of the main reasons for adoption of the Fourth Amendment was to provide citizens with the privacy protection necessary for secure enjoyment of First Amendment liberties. First Amendment values permeate the Fourth Amendment.").

[120] *See* Jameel Jaffer, *Surveillance and Its Impact on First Amendment Rights*, 57 AM. U. L. REV. 1224, 1225 (2008) ("[G]overnment surveillance can have a profound chilling effect on individuals' willingness to engage in activities that are protected by the First Amendment.").

[121] Solove, *supra* note 15, at 132. *But see* Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1383 (2008) (arguing that gap in Fourth Amendment doctrine is not filled by "importing First Amendment considerations").

[122] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).

cannot be outlawed by Congress.[123] Similarly, *NAACP v. Alabama* stands for the premise that the First Amendment prevents compelled disclosure of membership in an association, since the threat of disclosure may deter individuals from joining.[124] Deliberate efforts by the government to chill or undermine membership in political groups that embrace ideological views sympathetic to terrorism would thus run afoul of the First Amendment.[125]

However, as Part II.B.1 elaborates in further detail, the fundamental difficulty with relying on the First Amendment in the NSL context is that our Internet activity may not implicate First Amendment interests enough to trigger constitutional concerns about speech and association.[126] By extension, then, the data derived from that Internet activity may not be sufficiently linked to communication and association that an NSL, the purpose of which is ostensibly to aid a counterterrorism investigation, would create a cognizable chilling effect on protected activity.[127] Where the government is not seeking to regulate or prohibit political dissent, or to suppress a particular viewpoint about, for example, democracy or terrorism, the standard of review is relaxed, making a First Amendment challenge even more difficult.[128] The next sections look more closely at the hurdles a First

---

[123] *See id.* (emphasizing that, except under specific circumstances, First Amendment "do[es] not permit a State to forbid or proscribe advocacy of the use of force or of law violation"). The Patriot Act recognizes the importance of free speech and prohibits the use of an NSL solely for information related to First Amendment activity. 18 U.S.C. § 2709(b)(1) (2006). The problem, as Professor Schulhofer notes, is that an investigation is rarely undertaken *solely* on the basis of First Amendment activities, and thus this provision is empty rhetoric. SCHULHOFER, *supra* note 3, at 63.

[124] NAACP v. Alabama, 357 U.S. 449, 462, 466 (1958). For an analysis of the First Amendment implications of government surveillance, see generally Fisher, *supra* note 15.

[125] STONE, *supra* note 118, at 120.

[126] *See* Richards, *supra* note 18, at 428 (arguing traditional First Amendment doctrine underprotects activities not involving speech or writing).

[127] Litigants who challenge government actions based on their chilling of First Amendment activities face a significant hurdle in establishing the presence of a concrete harm. *See* Laird v. Tatum, 408 U.S. 1, 13–14 (1972) (holding that mere existence of Army's data-gathering program was insufficient to confer standing); ACLU v. NSA, 493 F.3d 644, 663, 665 (6th Cir. 2007) (holding that potential injury to plaintiff from suspicion of warrantless wiretapping "derive[d] solely from the fear of secret government surveillance" and therefore was not sufficiently concrete to establish standing); Phila. Yearly Meeting v. Tate, 519 F.2d 1335, 1337–39 (3d Cir. 1975) (dismissing claims that "mere police photographing and data gathering at public meetings" created anything more than "subjective chill" but noting that non–law enforcement use of information by broadcasting on television would create concrete chilling effect). A subscriber who wishes to challenge an NSL is likely to face the same difficulties. Further, unless an ISP successfully challenges a nondisclosure order, the subscribers themselves would have no knowledge of any information-gathering activities and thus would not have evidence to prove any substantial chilling effect in their electronic or telephone communications.

[128] *See infra* Part II.B.2.

Amendment challenge to government information gathering must clear.

1. The First Amendment's Relationship to Privacy

While the First and Fourth Amendments overlap in their historical origin,[129] they do not protect identical interests.[130] The critical question in a First Amendment challenge is the extent to which an NSL actually implicates free speech and association. The Fourth Amendment prevents unnecessary intrusions into a sphere that society recognizes as private; neither communication nor association need be present as a prerequisite. The amendments thus have different relationships to privacy.[131] Fourth Amendment privacy is, at root, about freedom from the scrutiny of others, and, in particular, from the government.[132] Its notion of privacy is more general, divorced from a particular goal, such as free speech.[133] In contrast, the First Amendment protects the liberty to interact with others through speech without fear of government suppression or reproach; only in rare instances does the First Amendment explicitly protect a right to be free from others.[134] In sum, the First Amendment protects what you say, whereas the Fourth Amendment prevents the government from listening in while you speak.

The Supreme Court has traditionally protected First Amendment freedoms even when the protected activities occur in private. Hence, in *Stanley v. Georgia*, the Court found viewing "obscene" material in one's home to be protected.[135] Indeed, as Solove notes, the reach of the First Amendment is not limited strictly to public spaces; since most political conversations take place between individuals in private

---

129 *See supra* notes 118–19 and accompanying text.

130 *See* STONE, *supra* note 118, at 119 (discussing different values at stake in each amendment); Solove, *supra* note 15, at 131 (noting amendments' differences).

131 Privacy is, of course, a nebulous concept. Solove argues that there are six general but overlapping categories: the right to be let alone, limited access to the self, secrecy, control over personal information, personhood, and intimacy. Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1092 (2002). My argument stresses only that the First and Fourth Amendments each bears a different relationship to privacy.

132 *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) ("At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." (citations omitted)).

133 *See, e.g.*, Katz v. United States, 389 U.S. 347, 351–52 (1967) (drawing distinction between Fourth Amendment's general right to privacy and other provisions of Constitution, such as First Amendment, that protect specific uses of privacy).

134 *See infra* notes 135–39 and accompanying text (discussing First Amendment's protection of privacy).

135 394 U.S. 557, 565 (1969) ("If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch.").

settings, private speech is not deprived of all First Amendment protection.[136] Neil Richards has recently argued that the First Amendment is concerned with "intellectual privacy," which he defines as "the freedom of the mind."[137] Put differently, one might say that the First Amendment protects "expressive privacy"—privacy that is designed to cultivate autonomy in furtherance of democratic debate, whereas the Fourth Amendment protects "intimate privacy."[138] The First Amendment *can* protect privacy, but it does so for the purpose of protecting forms of expression ultimately linked to public debate and political discussion—the values that the First Amendment attempts to foster.[139]

By protecting what society reasonably expects will remain private, the Fourth Amendment clears a space for disseminating thoughts and expression that the First Amendment safeguards directly. But the First Amendment's protection of that same private sphere is limited when the government is not directly attempting to regulate speech or association and is instead engaged in law enforcement activity. Further, the chilling effect doctrine can protect privacy only where doing so is necessary to safeguard speech. This is a key difference in how the two Amendments operate—the chilling effect doctrine requires proof that the government's action actually deters

---

[136] *See* Solove, *supra* note 15, at 121–22. Solove's focus on association suggests that privacy rights may receive more protection when coupled with associational activities, which are inherently public, than when part of private communication alone. *Id.* at 155 ("In freedom of association cases, the Court may be especially willing to find a chilling effect.").

[137] Richards, *supra* note 18, at 402. Richards notes the tension between privacy and the First Amendment, asserting that only on "rare occasion" has the Court extended the First Amendment doctrine to protect "the freedom of the mind." He argues that First Amendment *doctrine* only protects privacy "peripherally," *id.* at 401–02, but makes a compelling case that First Amendment *values* have a much stronger relationship to privacy.

[138] I draw a distinction analogous to that drawn by the Supreme Court in *Roberts v. U.S. Jaycees*—between "intimate association," or associating with others personally, and "expressive association," or associating with others to convey a message. 468 U.S. 609, 618, 622 (1984). *See* Fisher, *supra* note 15, at 637 (noting that the Court has distinguished "expressive" association from "intimate association," with the former being linked to public advocacy); *see also* Richards, *supra* note 18, at 403 ("[M]eaningful freedom of speech requires meaningful intellectual privacy."). Richards and I both treat privacy as a necessary predicate to expression and association, but I focus on privacy as a domain in which free expression circulates while Richards focuses on privacy as a space for developing the intellectual thought from which expression springs.

[139] Merely associating with others in private interaction does not trigger the First Amendment's protection of association. First Amendment doctrine protects association when a group collectively expresses a message; chilling membership can then affect the ability of the group to convey that message. The group's existence need not be for the purpose of expressing that message. *See* Boy Scouts of Am. v. Dale, 530 U.S. 640, 655 (2000) ("An association must merely engage in expressive activity that could be impaired in order to be entitled to protection.").

speech, whereas the Fourth Amendment's protection of privacy does not demand proof of any impact, since a plaintiff need only show that a recognized privacy interest will be infringed. The chilling effect doctrine thus implies a higher threshold for establishing a claim.

Recent case law on surveillance emphasizes the First and Fourth Amendments' differing relationship to privacy. In *ACLU v. NSA*, the Sixth Circuit demonstrated how judicial focus on the First Amendment as protective of public discourse—and not of privacy *qua* privacy—can influence judicial understanding of the chilling effect of government surveillance.[140] Plaintiffs' challenge to the NSA warrantless wiretapping program[141] alleged, inter alia, violations of the First and Fourth Amendments.[142] The Sixth Circuit, in denying the plaintiffs' claims, emphasized that the First Amendment protected *public* speech, whereas the Fourth Amendment was directed at protecting *privacy*: "[T]he First Amendment protects one's right to associate and be heard, while the Fourth Amendment protects the right to remain unheard. The First Amendment protects one's posting of a sign in her front yard, while the Fourth Amendment protects her hiding of the same sign in the basement."[143] Although the Sixth Circuit perhaps overstates the case, there is, nevertheless, a distinct *privileging* of public speech over private speech in First Amendment jurisprudence.[144]

The distinction is emphasized in the Supreme Court's balancing of competing speech interests in *Bartnicki v. Vopper*.[145] In that case, the Court held that the public's First Amendment interest in hearing an illegally recorded, private conversation about union negotiations outweighed the privacy rights of the union officials who had been illegally taped.[146] The Court recognized that privacy rights were essential

---

140 493 F.3d 644, 659–66 (6th Cir. 2007).

141 The Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended in scattered sections of 8, 18, and 50 U.S.C.).

142 493 F.3d at 649–50.

143 493 F.3d at 657 n.15.

144 *See* Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 987 (2003) (arguing that First Amendment protects speech "of public concern" more than speech of purely private concern). However, the Court has privileged privacy interests over public speech when alternative outlets for public speech existed. In *Frisby v. Schultz*, 487 U.S. 474 (1988), for example, the Court upheld an ordinance that prevented picketing in front of a residential home based on the privacy of the home and the availability of alternative channels of public protest.

145 532 U.S. 514 (2001).

146 *Id.* at 534–35. In the case, negotiations took place between teachers and a local school board over a collective bargaining agreement, which culminated in a proposal considered favorable to the teachers. An unidentified individual intercepted a private call between the union negotiator and the union president discussing the negotiations. On his radio program, Vopper played the tape, on which the negotiator mentioned the need to

to the union officials' First Amendment freedom and that public disclosure of private conversations might have a chilling effect. Nonetheless, it held that the collective public interest in the information was more important, asserting that "privacy concerns give way when balanced against the interest in publishing matters of public importance."[147] Thus, the First Amendment's privacy concern is secondary to its concern with fostering public debate.

The *Doe I* court's treatment of the third-party doctrine underscores how the same information may be treated differently by each Amendment. The court rightly rejected the government's argument that the *First* Amendment did not protect anonymous Internet expression or association because the information had been voluntarily given to a third party.[148] This argument conflated the two amendments and their respective relationship to privacy. Although the Fourth Amendment does not find a reasonable expectation of privacy in information given to third parties, the First Amendment may still protect expressive interests in that information.[149] Consider, for example, that although membership lists are held by third parties, they are not deprived of First Amendment protection.[150] Thus, the court's distinction reiterates that the *Fourth* Amendment provides a space for self-development—privacy itself has value without any need for reference

---

"go to [the school board members'] homes . . . [t]o blow off their front porches." *Id.* at 518–19. The public nature of the negotiations made the private conversation newsworthy. *Id.* at 525.

147 *Id.* at 534. In contrast, the dissenting opinion by Chief Justice Rehnquist emphasized privacy interests. He found that the criminalizing statute was a content-neutral restriction, focused only on the manner of acquisition of the information and not on the importance of the subject matter. *Id.* at 547–49 (Rehnquist, C.J., dissenting).

148 Doe v. Ashcroft (*Doe I*), 334 F. Supp. 2d 471, 508 (S.D.N.Y. 2004). *But see* Reporters Comm. for Freedom of the Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1058 (D.C. Cir. 1978) ("To the extent individuals desire to exercise their First Amendment rights in private, free from possible good faith law enforcement investigation, they must operate within the zone of privacy secured by the Fourth Amendment.").

149 *Doe I*, 334 F. Supp. 2d at 508 ("No court has adopted the Government's argument here that anonymous internet speech or associational activity ceases to be protected because a third-party ISP is in possession of the identifying information.").

150 *See In re* First Nat'l Bank, 701 F.2d 115, 118 (10th Cir. 1983) (affirming viability of challenge to bank's disclosure of organization members' records on ground that right to free association "will be chilled equally whether the associational information is compelled from the organization itself or from third parties"); *see also* Strandburg, *supra* note 15, at 793 (arguing that, to trump right of free association, organization must be implicated in government purpose and obtaining membership list must be necessary to effectuate that purpose). An organization with an official webpage or email account would have a stronger claim that disclosure would have a chilling effect because the electronic data might reveal its membership.

to a public sphere.[151] Under the First Amendment, in contrast, privacy remains connected to the need for an autonomous space that serves as a predicate for participation in a public sphere of debate and discourse.[152] Although the third-party doctrine says that we assume the risk that our information may be revealed, the First Amendment may still protect a certain expectation of privacy so that speech and association will not be unduly chilled. Thus, the First Amendment has the potential to protect information that the third-party doctrine does not.

In the NSL context, the critical inquiry then becomes when the threat of disclosure of the information sought is deemed to have a chilling effect on protected speech or association—that is, when "expressive privacy" is impacted.[153] As *Doe I*'s analysis suggested, government access to electronic communication transactional records (ECTRs) might chill subscribers' willingness to engage in protected communication.[154] Yet other courts may find that the information the government seeks is not sufficiently tied to First Amendment activity to trigger protection, either by relying on a public-private divide—as in *ACLU v. NSA*[155]—or simply by finding that, even in the Internet context, not all the data sought by an NSL implicates First Amendment values.[156] Financial data and records concerning sources of payment of ISP fees, for example, do not directly concern speech and thus may not trigger First Amendment concerns.[157]

---

151 *See* SCHULHOFER, *supra* note 3, at 65 ("[T]he central value of the Fourth Amendment [is] the right to preserve a private space in which people are free to grow, explore, or simply be themselves.").

152 There is a tension in First Amendment jurisprudence between the value of public discourse—in which the free flow of ideas is at the core of the freedom of expression—and the privacy necessary to formulate and protect those ideas. For a thoughtful discussion, see Franklyn S. Haiman, *Speech v. Privacy: Is There a Right Not To Be Spoken To?*, 67 Nw. U. L. REV. 153, 154 (1972) ("The issue of whether there is a right to be free *from* speech poses a sharp conflict between freedom of speech, on the one hand, and privacy on the other."). *See also* Solove, *supra* note 144, at 1000 (arguing that, in its jurisprudence on tort of public disclosure, Court has laid out distinction between public and private speech more clearly than in constitutional cases).

153 *See* Richards, *supra* note 18, at 428 (emphasizing need to look at implications of government activity on First Amendment values); Solove, *supra* note 15, at 151–59 (same).

154 *Doe I*, 334 F. Supp. 2d at 511–12.

155 *See supra* note 140.

156 Even Solove recognizes that a chilling-effect analysis "will depend upon the specific facts of each case, including whether the person being investigated can demonstrate deterrence of First Amendment activities." Solove, *supra* note 15, at 156.

157 *See, e.g.*, *Doe I*, 334 F. Supp. 2d 471, 509 (S.D.N.Y. 2004) (conceding that *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), might be used to imply absence of First Amendment protection for customer records from telephone companies and banks).

Consider how a court might treat the information sought by an NSL that potentially implicates First Amendment values. Obtaining lists of email "envelope information"—i.e., the number of emails sent and their recipients, dates, and subject lines—is unlikely to threaten anonymous speech, since most such communications are not anonymous in the first place. Nor does such disclosure necessarily impact the right of free association because such emails may not be sent in the context of a collective group.[158] As a result, a court might be skeptical that conveying this information to the government actually chills communicative activity. Similarly, revealing metadata and IP addresses does not infringe on anonymity if the websites involved do not allow anonymous emails, postings, or chat rooms. Even the disclosure of search queries, which reflect a user's reading habits and intellectual life, and which may deprive him of the right to receive information anonymously, may not be found to chill activity: While the NSL statute requires that the information be "relevant" to an "authorized investigation,"[159] it does not guarantee that the information gathered will actually be used against the subscriber in a criminal proceeding, thus making it harder to establish a chilling effect.[160] Even if any of this data is found to implicate protected speech, protection of that speech still would be balanced against the government's competing interest, a topic explored in the next section.

2. Standards of Review

The foregoing analysis suggests that, under the First Amendment, a litigant faces two challenges. Not only must she prove that her communicative or associative activities are concretely chilled, but she must also establish that those activities fall within the scope of First Amendment protection and are not of a purely private nature. The subscriber's privacy rights, however, even if protected by the First Amendment, are not absolute. A brief analysis of the balancing required in the NSL context shows that a court could easily find the compelling interest in national security to outweigh the subscriber's interest in the privacy of Internet activity data.

Under contemporary First Amendment doctrine, when the government seeks to regulate expression or association in a manner unre-

---

158 This recalls the distinction made between expressive and intimate association from *Roberts v. U.S. Jaycees*. *See supra* notes 138–39 and accompanying text; *see also* Strandburg, *supra* note 15, at 768–69 (arguing that surveillance law cannot protect associative interests until it moves beyond privacy-based paradigm).

159 18 U.S.C. § 2709(b)(2) (2006).

160 *But see* Solove, *supra* note 15, at 166 (positing scenario in which government seeks Internet search records for criminal proceeding).

lated to the message or viewpoint, such content-neutral regulation is subject to a more deferential mode of scrutiny that balances the government's interest with the individual's freedom of expression.[161] The deference given to the government is even greater when the statute does not regulate expressive activity directly but has only an incidental effect on speech or association.[162] In *United States v. O'Brien*, for example, the Court upheld the application of a prohibition on burning draft cards against the defendant, who burned his draft card in public protest of the draft.[163] The government's legitimate interest in the efficient administration of the Selective Service was held to outweigh O'Brien's expressive interest in burning his draft card as a political protest. The fact that he had alternative means of expressing his political views bolstered the government's case.[164] Similarly, in *Roberts v. United States Jaycees*, the Court addressed the application of an antidiscrimination statute to a nonprofit group that excluded women from regular membership.[165] The Court held that requiring the organization to permit women to join would not undermine its associative interests.[166] In doing so, the Court established that burdens on rights of association are permissible when the government has a compelling interest unrelated to the suppression of ideas that cannot be achieved through significantly less restrictive means.[167]

Government issuance of NSLs is potentially subject to this more deferential standard of review. The use of NSLs likely falls within the content-neutral category of regulation, imposing only an incidental effect on speech.[168] And, in contrast to the NSL gag order, which directly targets speech on a particular topic,[169] the government's

---

161 Content-neutral regulations do not restrict speech on the basis of viewpoint or subject matter. *See, e.g.*, Roberts v. U.S. Jaycees, 468 U.S. 609, 623 (1984) (noting that challenged statute "does not distinguish between prohibited and permitted activity on the basis of viewpoint"). *See also* Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46, 48 (1987) ("Content-neutral restrictions limit expression without regard to the content or communicative impact of the message conveyed.").

162 An incidental restriction exists when a law of general applicability has the inadvertent effect of suppressing speech although it is not directed at speech. In these cases, courts employ a balancing test that is deferential to the government. *See, e.g.*, United States v. O'Brien, 391 U.S. 367 (1968) (upholding prohibition on burning draft cards).

163 *Id*.

164 *Id.* at 381–82.

165 468 U.S. at 614.

166 *Id.* at 623, 627.

167 *Id.* at 623.

168 For an argument that a similar, intermediate standard of review would apply to a hypothetical "Orwellian" surveillance law, see generally Lynch, *supra* note 18.

169 The First Amendment rights of the ISPs enjoyed the strongest standard of review in *Doe I* and *Doe III*: The district courts treated the gag order as a content-based restriction subject to strict scrutiny because it excluded a particular topic—receipt of the NSL—from

request for information is arguably an incidental restriction on the subscriber's speech—the chilling effect is not its primary purpose. Although the chilling effect may be quite strong, the government's ostensible purpose is content-neutral insofar as it seeks not to regulate any particular viewpoint or subject matter but rather to gather information for legitimate law enforcement purposes.[170] Further, as we have seen, some of the information requested may not be expression at all: Data regarding payment plans, financial records, and even IP addresses are not necessarily speech.

On the other hand, the situation is not clear cut, and there is ample room to debate whether the government's pursuit of Internet data regulates expression; the government, after all, is targeting speech-related activity. In an as-applied challenge, for example, a litigant could argue that the NSLs have been, up to that point, directed primarily at political viewpoints that express anti-American sentiment or extol the values of terrorism as a political tactic. The government might assert in response that this characterization is too broad and that it seeks communications and Internet activity tied to terrorist activity. This aim, the ostensible purpose of the NSL, is content-neutral, related to the evidentiary value of the information and not its expressive dimension. Thus, if the litigant cannot prove that he was targeted for his particular viewpoint, the more deferential standard likely will be applied.

Another recent case, *Tabbaa v. Chertoff*, demonstrates how this deferential review might favor the government's interest in national security.[171] There, the Second Circuit found that searches and six-hour border detentions of plaintiffs, U.S. citizens who were Muslim and had attended a conference on Islam abroad, did not violate the First or Fourth Amendment. Although the detentions were found to have a substantial chilling effect on the right to free association, the court, applying the test from *Roberts v. United States Jaycees*,[172] found

---

public debate. *See* Doe v. Gonzales (*Doe III*), 500 F. Supp. 2d 379, 397 (S.D.N.Y. 2007) (reiterating *Doe I*'s conclusion that § 2709(c) "functioned as a content-based restriction because it closed off an 'entire topic' from public discourse" (quoting Doe v. Ashcroft (*Doe I*), 334 F. Supp. 2d 471, 513 (S.D.N.Y. 2004))). On appeal, the Second Circuit panel was divided and contemplated a lesser standard, noting that the nondisclosure requirement of § 2709(c) is not "a typical content-based restriction" and that the category of information required to be held confidential is "a narrow one." John Doe, Inc. v. Mukasey (*Doe IV*), 549 F.3d 861, 877–78 (2d Cir. 2008).

170 *See, e.g.*, Fisher, *supra* note 15, at 645 (arguing that surveillance for antiterrorist purposes that has incidental effect on First Amendment expression should be analyzed under "more lenient" *O'Brien* test).

171 509 F.3d 89 (2d Cir. 2007).

172 468 U.S. at 623 ("Infringements on [the right to associate for expressive purposes] may be justified by regulations adopted to serve compelling state interests, unrelated to the

the government's interest in protecting the nation from terrorism to be compelling and detention at the border to be narrowly tailored, as it is the most effective means of preventing suspected terrorists from entering the country.[173] *Tabbaa* suggests that, under such a balancing test, national security is likely to trump an individual's First Amendment claim that government information gathering has a chilling effect.

Litigants who challenge the government's use of NSLs may face similar difficulties. Although *Doe I* found that the use of NSLs could potentially chill protected activity,[174] another court could find that the government's compelling interest in national security outweighs the privacy interests in anonymous speech or expressive association. The government might argue that, due to the covert nature of terrorism, no less restrictive alternative exists that would allow it to obtain information quickly enough to dispel plots prior to their realization.[175] Even if the NSL sought First Amendment–protected information, the government's interest in protecting national security could likely trump privacy interests in anonymous speech in chat rooms or email communications of an association; alternative means of engaging in free expression are available.

A litigant might still try to argue in some instances that the use of an NSL is not sufficiently narrowly tailored because it lacks procedural safeguards to guarantee that the NSL process properly balances security and speech interests.[176] After all, in *Doe IV*, the Second Circuit emphasized the need for judicial review to ensure that the ISP's free speech interests were not unduly burdened by the nondisclosure

---

suppression of ideas, that cannot be achieved through means significantly less restrictive of associational freedoms.").

173 509 F.3d at 102–03. The court credited the government's assertion that it had specific intelligence that the conference would be a "possible meeting point for terrorists to exchange ideas and documents." *Id.* at 103 (quoting intelligence received by Bureau of Customs and Border Patrol officials).

174 The *Doe I* court declined to determine the scope of a subscriber's First Amendment rights, limiting itself to finding that § 2709 could reach large quantities of protected speech in the absence of any judicial review provision. *See* Doe v. Ashcroft (*Doe I*), 334 F. Supp. 2d 471, 506, 509 (S.D.N.Y. 2004).

175 Solove cites lower court decisions that have imposed higher standards for subpoenas of Internet information that would reveal the identity of users and thus eliminate anonymity, but none of those cases involved terrorism or national security where arguably the government's interest could meet a heightened burden. *See* Solove, *supra* note 15, at 145–46 & n.189 (surveying case law).

176 Under the *O'Brien* test, the court considers whether the incidental restriction on speech is "no greater than is essential," but it need not be the least restrictive alternative. United States v. O'Brien, 391 U.S. 367, 376 (1968). Under *Roberts*, the government must show that its interest cannot be achieved through significantly less restrictive means. 468 U.S. at 623.

provision. Although the current judicial review provision for challenging production, § 3511(a), might be deemed sufficient to protect First Amendment interests, a court could find that, because the ISP has little incentive to move to quash the request, the subscriber should have some additional procedural safeguard to ensure that the information is "relevant" to a government investigation.[177] A court could thus require some sort of judicial review provision initiated by the subscriber. Nevertheless, the balance struck will probably favor the government, since, as *Doe IV* demonstrates, a court is unlikely to impose an ex ante review process, even if it applies a standard close to strict scrutiny.[178]

III
An Assessment of the Possible Solutions

The First Amendment currently plays a crucial yet insufficient role in safeguarding against information gathering that might chill an individual's Internet communications. The First Amendment does not provide full protection for all confidential information, and the current standards seem to favor the government's interest in national security. These limitations suggest that, instead of attempting to establish a claim that the NSLs chill speech, we should address directly, by means of the Fourth Amendment, the privacy concerns that all NSLs implicate. Such protections can provide concomitant benefit to First Amendment interests.

In engaging in the analysis, we must first decide whether we are concerned solely with First Amendment values or if we value privacy more generally. It is certainly plausible to argue that open debate should be protected more strongly than financial data, since the former is an essential check against government in a way that the latter is not. Yet it is difficult to deny that we retain some expectation of privacy in data provided to certain third parties, and as such our interest in privacy is not limited to speech and association.[179] We may therefore need to rethink the third-party doctrine's assumption that information we provide to third parties is no longer private.[180]

This Part considers both statutory and constitutional measures that could alleviate concerns about privacy from government informa-

---

[177] 18 U.S.C. § 2709(b)(1) (2006).

[178] *See supra* notes 110–11 and accompanying text.

[179] *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1122 (2002) ("[Privacy] is also implicated where information relates to issues of our most basic needs and desires: finances, employment, entertainment, political activity, sexuality, and family.").

[180] On the third-party doctrine, see *supra* notes 44–47 and accompanying text.

tion gathering. Commentators have suggested two general solutions to the problems of government information gathering: (1) revising the Patriot Act to include additional safeguards, and (2) revising the third-party doctrine so that it actually extends Fourth Amendment protection to information held by certain third parties.[181] This Part considers the value of each approach by exploring the interest it protects and the balance it strikes between citizens' privacy interests and the government's legitimate law enforcement and national security needs.

A. Expanding Statutory Protections

The most direct solution to the privacy problems created by NSLs is to amend the statute so that it provides better safeguards.[182] Congress could extend protection to all data that society might consider private, including financial records, or tailor the statute to ensure that, at a minimum, it protects Internet activity that implicates the First Amendment. Various other reforms of the Patriot Act have been suggested, including more rigorous reporting requirements,[183] more precise statutory definitions,[184] and expanded judicial review.[185] Of these, the ex ante involvement of a detached and neutral arbiter is the mechanism most likely to guarantee that the proper balance of interests is being met.[186] Reporting requirements operate ex post,

---

[181] I do not offer a reform of First Amendment doctrine to accommodate information-gathering claims. See Lynch, *supra* note 18, for a proposal to reform First Amendment doctrine based on the right to choose one's audience.

[182] *See, e.g.*, SCHULHOFER, *supra* note 3, at 74–78 (providing overview of suggested statutory reforms).

[183] The Attorney General is now required to submit semiannual reports to Congress detailing the number of NSLs issued. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 118(f)(1), 120 Stat. 192, 218 (2006) (codified as amended at 18 U.S.C. § 3511 (2006)). Nevertheless, the numbers alone do not provide a complete picture of the FBI's activities. See SCHULHOFER, *supra* note 3, at 74–75, for an argument that Congress should receive semiannual reports detailing "essential details" such as the particular types of institutions targeted for NSLs and the particular categories of information requested (e.g., communication records).

[184] Congress should amend § 2709 to include a more precise definition of "ECTR" in order to ensure that that an ISP provides no more information than is necessary for the government to conduct its investigation. *See* Shankman, *supra* note 22, at 262 (noting need for more precise statutory definition).

[185] Some scholars advocate for more public accountability through the use of a case-by-case approach to the nondisclosure "gag order." *See, e.g.*, SCHULHOFER, *supra* note 3, at 75–76; *see also* Shankman, *supra* note 22, at 263.

[186] *See* SCHULHOFER, *supra* note 3, at 76–77 (arguing that "[a] central premise of the Fourth Amendment" is requirement of ex ante review before neutral magistrate instead of just relying on "police officer's good-faith determination of the facts"); Raab, *supra* note 10, ¶ 47 (advocating ex ante justification before judge); Strandburg, *supra* note 15, at 816–18 (urging that surveillance of communications traffic data be authorized ex ante by court order).

informing Congress of what has already occurred, and thus have limited capacity to deter present abuses. More precise statutory definitions will aid the court in its review process, but only judicial review can overcome the problems of self-certification that enable the FBI to overreach.[187] The judicial review procedures must balance the legitimate government interest in combating terrorism with individual privacy concerns, but they can easily be tailored to avoid placing an undue burden on the government.

Although the involvement of a neutral and independent magistrate theoretically will deter unwarranted use of NSLs,[188] additional safeguards are needed in order to prevent overreaching and ensure adherence to statutory guidelines. A requirement that an FBI agent provide assurance that the information sought is relevant to an investigation is insufficient to perform this function, as the agent clearly has an incentive to assert relevance even where the connection between the investigation and the requested information is tenuous or nonexistent. A process akin to that of the Foreign Intelligence Surveillance Act (FISA) would be more effective in balancing the needs of national security against privacy and speech concerns.[189] FISA requires the government to submit a request for a court order to the Foreign Intelligence Surveillance Court (FISC), created specifically to handle requests to undertake government surveillance for counterintelligence purposes.[190] The safeguard provided by ex ante judicial review would be further enhanced by returning to the original stan-

---

This is not to say that judicial review of such requests is always effective. *See, e.g.*, Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 34 (1988) (discussing magistrates' "rubber stamp[ing]" of warrant requests). Nevertheless, the premise of the warrant requirement is that some form of judicial oversight will deter overreaching. *See* Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971) (describing warrant requirement as "an important working part of our machinery of government, operating as a matter of course to check the 'well-intentioned but mistakenly over-zealous executive officers' who are a part of any system of law enforcement" (citation omitted) (quoting Gouled v. United States, 255 U.S. 298, 304 (1921))).

187 The *Doe III* court summarized the various standards that the government must meet ex ante to acquire a wiretap, install a pen register or trap-and-trace device, or obtain a court order to produce contents of communications. Although those standards fall along a spectrum, they nevertheless all require some form of ex ante judicial approval. Doe v. Gonzales, 500 F. Supp. 2d 379, 392–94 (S.D.N.Y. 2007).

188 *See* Wasserstrom & Seidman, *supra* note 186, at 34 (discussing impact of rubber-stamping problem on quality of magistrate review).

189 For similar appraisals of potential changes to the Patriot Act, see SCHULHOFER, *supra* note 3, at 77; Shankman, *supra* note 22, at 261–64. As further encouragement, recent data has revealed that the FISC, which oversees FISA requests, is not solely a rubber-stamp body. SCHULHOFER, *supra* note 3, at 43.

190 Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1803, 1804 (2006).

dard of "specific and articulable facts."[191] These changes would better protect information held by third parties, thus ameliorating the limitations of both the First and Fourth Amendments.

B. Modifying the Third-Party Doctrine

On the constitutional front, the Fourth Amendment third-party doctrine could be revised to account for the proliferation of Internet communication.[192] The third-party doctrine has already come under considerable fire from a number of scholars;[193] seminal cases on the issue have been assailed as out of touch with what society perceives to be a reasonable expectation of privacy in data conveyed to

---

[191] In 2007, Senator Russell Feingold introduced the National Security Letter Reform Act, S. 2088, 110th Cong. (2007), which would have made a number of these changes for NSLs that seek communications-related information. It required that information like phone numbers dialed could be obtained only through the FISC or grand jury subpoena. *See id.* § 2 (amending 18 U.S.C. § 2709(a)(2)). The bill reestablished the "specific and articulable facts" standard and provided an individual with a mechanism by which to challenge the information gathering if the data is to be used in a criminal proceeding. *See id.* § 2 (amending 18 U.S.C. § 2709(b)(1)(B), (f)). The Senate Judiciary Committee held hearings in April 2008, but no further progress was made. In March 2009, Representatives Jerrold Nadler and Jeff Flake introduced a similar bill. National Security Letters Reform Act of 2009, H.R. 1800, 111th Cong. (2009). Despite the bill's recent introduction, it remains unclear what will happen to the demand for reform of the NSL process during the Obama administration. The administration, for example, decided not to appeal the Second Circuit's decision in *Doe IV*. *See* Press Release, Am. Civil Liberties Union, Obama Administration Will Not Ask Supreme Court To Take Up National Security Letter "Gag Order" Decision (May 18, 2009), *available at* http://www.aclu.org/safefree/nationalsecurity letters/39605prs20090518.html.

[192] Richards concurs in the idea that First Amendment doctrine may not be able to support the need for protection from government surveillance and calls for rethinking the third-party doctrine. *See* Richards, *supra* note 18, at 428, 431. He does not elaborate at length on how the First or Fourth Amendment should be retooled to protect that privacy; he argues only that current jurisprudence leaves intellectual privacy vulnerable. *Id.*

[193] *See, e.g.*, Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1403, 1407 (2004) (arguing that *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), do not "foreclose any claim of an expectation of privacy in communications held by a service provider" and that such an argument is "doctrinally and normatively unsound"); Brenner & Clarke, *supra* note 53, at 245–46 (listing ways third-party doctrine is analytically flawed); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) ("The third-party doctrine is the Fourth Amendment rule scholars love to hate. It is the *Lochner* of search and seizure law, widely criticized as profoundly misguided." (citation omitted)); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1591–92 (2004) (claiming existence of expectation of privacy in email because service provider is not "recipient"); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005) ("The third party doctrine presents one of the most serious threats to privacy in the digital age.").

intermediaries like financial institutions or ISPs.[194] Although the third-party doctrine appears to be well settled,[195] modifying it could guarantee the privacy of a significant amount of data, dramatically expanding the scope of Fourth Amendment protections.[196] Buttressing privacy claims through the Fourth Amendment would, in turn, provide additional protection to First Amendment activities undertaken through the Internet.[197]

Rather than attempt to expand the First Amendment by importing Fourth Amendment requirements and procedures,[198] we ought to build on the Fourth Amendment's traditional relationship to the First Amendment by allowing their overlap to push Fourth Amendment standards in a more exacting direction.[199] Courts could thus begin to reformulate the current Fourth Amendment reasonable expectation of privacy test to more directly incorporate First Amendment values,[200] considering them when evaluating both the subjective and objective prongs of the *Katz* expectation of privacy test.[201] Liti-

---

194 Brenner & Clarke, *supra* note 53, at 252 (arguing that *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), are difficult to reconcile with modern expectation of privacy in machine-human transactions).

195 STONE, *supra* note 118, at 142 (describing third-party doctrine as "settled law").

196 *See* Brenner & Clarke, *supra* note 53, at 266–73 (positing "relation-based" theory of privacy in which transfer of data is not equivalent to voluntary "disclosure" that assumes risk). For a proposal that would require the police to have probable cause before they could obtain any third-party information held in a "system of records," see Solove, *supra* note 179, at 1162.

197 *See* Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978) ("Where presumptively protected materials [under the First Amendment] are sought to be seized, the warrant requirement [under the Fourth Amendment] should be administered to leave as little as possible to the discretion or whim of the officer in the field."); *see also supra* notes 118–20 and accompanying text (discussing how Fourth Amendment warrant requirement can safeguard First Amendment free speech rights).

198 *E.g.*, Solove, *supra* note 15, at 163 ("[T]he lack of a textual basis under the First Amendment should not preclude importing warrants, probable cause, the exclusionary rule, and other concepts from the Fourth Amendment [to the First Amendment].").

199 *See supra* notes 118–20 and accompanying text.

200 Richards, *supra* note 18, at 440. Solove, *supra* note 15, at 131–32, considers a similar path, but pursues instead reliance on the First Amendment as an independent claim. Akhil Amar has argued for incorporating First Amendment values in the determination of the reasonableness of a search under the Fourth Amendment. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 806 (1994).

201 *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (observing "twofold requirement" that person have exhibited actual expectation of privacy and that expectation be reasonable). Richards points to the possibility of relying on content to expand Fourth Amendment protections, but he suggests that the potential for rethinking *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), lies in the First Amendment values at stake without developing the doctrinal argument. *See* Richards, *supra* note 18, at 439 (noting relevance of *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008), for rethinking third-party doctrine). I undertake that task here. *See also* Susan N. Herman, *The USA*

gants seeking to bolster Fourth Amendment protection in this field might, for example, urge the court to modify the third-party doctrine to find a *diminished* but still substantial expectation of privacy.[202]

While no court has extended Fourth Amendment protection to information held by third parties, a recent court of appeals case offered an analysis of the third-party doctrine's treatment of email that perhaps provides an opening for a more robust Fourth Amendment check on information gathering.[203] In *Warshak v. United States*, the Sixth Circuit held that email authors retain a reasonable expectation of privacy in the content of email, even once it is routed through an ISP's servers.[204] The panel likened email to telephone conversations and the contents of letters, neither of which can be accessed by the phone company or postal service and transmitted to the government under the third-party doctrine.[205] In doing so, the court rejected the government's argument that, because the ISP administrators would have occasional need to access users' emails in the course of managing the system, users lost their reasonable expectation of privacy. The court found that, "[b]ecause the ISPs [sic] right to access e-mails under [the] user agreements is reserved for extraordinary circumstances . . . , it is . . . insufficient to undermine a user's expectation

---

PATRIOT Act and the Submajoritarian Fourth Amendment, 41 HARV. C.R.-C.L. L. REV. 67, 120 (2006) ("It is plausible that the Court might distinguish *Miller* and *Smith* and find a reasonable expectation of privacy . . . , perhaps on the ground that specially protected areas are involved—areas implicating First Amendment freedoms, like activity on the Internet or in libraries." (citation omitted)).

202 For a proposal to vary the level of Fourth Amendment protection of third-party information based on whether the information is held by public or private entities, involves content or transactional data, and seeks information related to specific individuals, see Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 167–68 (2005). For a comparison of Solove and Slobogin's approaches in light of a series of relevant factors that courts ought to consider, see Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975 (2007).

203 Warshak v. United States (*Warshak I*), 490 F.3d 455 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008); *see also* Stephen E. Henderson, *Learning from All Fifty States: How To Apply the Fourth Amendment and Its State Analogs To Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 (2006) (surveying state constitutional decisions interpreting their state analogues to Fourth Amendment and finding that number of them reject idea that there is no reasonable expectation of privacy in information given to third parties); Slobogin, *supra* note 202, at 189–90 (arguing that *Ferguson v. City of Charleston*, 532 U.S. 67, 79 (2001), in the "special needs" doctrine signals Court's hesitancy to deny Fourth Amendment protections to all information given to third parties).

204 *Warshak I*, 490 F.3d at 473.

205 *Id.* at 471 ("Like telephone conversations, simply because the phone company or the ISP could access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course." (emphasis omitted)).

of privacy."[206] At first glance, then, drawing the line at email would seem to hew to the standard distinction between communication, on the one hand, and information given to third parties on the other.

What is important about *Warshak* is not what it does but rather what it *does not* do: On the logic of the third-party doctrine, the panel could have fit email content squarely within the third-party doctrine, denying subscribers an expectation of privacy in that content. Instead, the panel found that the ISP's privacy policy created some reasonable expectation of privacy.[207] The court rightly recognized a difference between the assumption of risk that the recipient of one's communications might divulge them and the expectation of privacy that attaches when the communications are conveyed through an "intermediary" like an ISP or phone company, which simply acts as a conduit.[208] It concluded that the reasonable expectation of privacy in that content was not destroyed by mere use of a third party's server.[209]

Although the decision was vacated by a rehearing en banc that found the case was not ripe for adjudication,[210] its reasoning might, potentially, be the first sign of a shift in how courts conceptualize the third-party doctrine for electronic communications. Courts are beginning to recognize that electronic communication poses a different set of problems. In the future, more courts may be willing to extend the expectation of privacy to "envelope information" that, in the case of the URLs that include search terms, may also contain some content.[211] Our sense that privacy is affected may be correlated with how

---

[206] *Id.* at 474.

[207] The terms of service allowed access to email content in limited situations, such as for enforcing the terms of service, responding to requests for customer service, and managing claims that the user had violated the rights of another user. *Id.* at 474 n.7.

[208] *Id.* at 471.

[209] *Id.* at 473.

[210] Warshak v. United States (*Warshak II*), 532 F.3d 521 (6th Cir. 2008) (en banc).

[211] There is hope for privacy interests in the content of electronic information despite the fact that the Sixth Circuit maintained a lack of expectation of privacy in "records and subscriber information," *Warshak I*, 490 F.3d at 474; *see also* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (holding that Internet users have no expectation of privacy in email addressees or websites visited). Federal legislation continues to recognize privacy interests in communication-related information provided to third parties. *E.g.*, Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, 120 Stat. 3568 (2007) (codified at 18 U.S.C. § 1039) (making criminal act of impersonating someone to obtain call records). The D.C. Circuit has upheld restrictions on communications providers sharing customer call data with third-party marketing partners because customers have a privacy interest in that data. Nat'l Cable & Telecomm. Ass'n v. FCC, 555 F.3d 996, 1001–02 (D.C. Cir. 2009); *see also* Bellia, *supra* note 193, at 1387 ("If positive law protects the privacy of communications, . . . then it becomes more reasonable to expect privacy in such communications.").

much of the content of our communications is exposed in envelope information.

Data that is more likely to implicate First Amendment values could receive more robust protection.[212] Financial data, for example, might not trigger concerns about First Amendment values to the same extent as personal data, like recipients and subject lines of emails.[213] Courts could therefore tailor their inquiries to recognize that envelope information in electronic communication is subject to a higher expectation of privacy, given the content contained within email subject lines and search queries. Relatedly, we might find that the aggregate data produced by a single user's online transactions is sufficiently private to warrant protection.[214] A compilation of the URLs of websites visited by a subscriber, for example, which collectively capture that individual's intellectual life, would merit heightened Fourth Amendment protection.[215] Sources of payment, lacking the same level of content, however, might not.

Such an approach finds support in Fourth Amendment doctrine. While it is true that the First Amendment may not expand the Fourth Amendment beyond the requirements of probable cause and a warrant,[216] the Court has never held that the First Amendment could not force a heightening of Fourth Amendment protections that otherwise would *fall below* the warrant requirement.[217] Because the First Amendment depends on a certain level of privacy to enable the exer-

---

212 *See* Slobogin, *supra* note 202, at 178–79, 182 (arguing that target-based transactional surveillance that touches on First Amendment issues should require higher standard than Patriot Act's "relevance" standard).

213 *See* Zittrain, *supra* note 34, at 88 (suggesting that low level of Fourth Amendment protection granted in financial records cases should not be extended to all third-party holding of private information). *But see* Solove, *supra* note 15, at 172–73 (discussing cases where courts found financial records implicated associations' First Amendment rights).

214 *See* Brenner & Clarke, *supra* note 53, at 251–52 (discussing difference between transactional data and voluntarily disclosed information).

215 At the same time, heightening the Fourth Amendment standard only when First Amendment values potentially are implicated may require drawing a difficult line; all surveillance and investigation may implicate or chill speech and association, and a more fine-grained approach to NSL requests might prove administratively burdensome.

216 Some have argued for a standard higher than the warrant standard when expressive interests are implicated. *See, e.g.*, Richards, *supra* note 18, at 434. The Supreme Court rejected this approach in *Zurcher v. Stanford Daily*, 436 U.S. 547, 565 (1978).

217 *But see Zurcher*, 436 U.S. at 565 (asserting that First Amendment only requires that "the courts apply the warrant requirement with particular exactitude when First Amendment interests would be endangered"). Amar notes that *Zurcher* permits this Note's suggestion of applying heightened Fourth Amendment standards to account for First Amendment concerns where the warrant requirement would not otherwise be mandated. Amar, *supra* note 200, at 806 ("First Amendment concerns could well trigger special Fourth Amendment safeguards [such as] heightened standards of justification prior to searching . . . .").

cise of free speech and association, the First Amendment might require that the Fourth Amendment floor be raised for data that implicates such concerns. Although First Amendment activities might not be impacted directly enough to support a cognizable First Amendment challenge, the potential effect on privacy as an essential cognate to First Amendment interests might nonetheless justify revision of the third-party doctrine.[218] The underlying presumption here is that the Fourth Amendment standards already incorporate a respect for the First Amendment.[219] Yet courts have not adequately questioned whether the presumptions underlying the third-party doctrine are properly extended to Internet data, which tend to contain more content than other "disclosed" communications.[220] It is the beginning of this inquiry, although unstated, that seems to drive the *Warshak* case.

In the absence of the third-party doctrine, government information gathering through NSLs would likely need to rely on a warrant issued on probable cause.[221] Nevertheless, some might argue that requiring a warrant, particularly for third-party information needed for counterintelligence purposes rather than criminal prosecution, might impose too onerous a burden on the government, tipping the scales too far in favor of privacy. Instead, following Slogobin's cue, courts could adopt a reasonable suspicion standard in which the FBI must, ex ante, provide a judge with specific and articulable facts that the individual's data is of material importance to an authorized investigation.[222] Relying on such a standard would impose heightened protection that balances the prospective needs of counterintelligence activities with the privacy interests in information held by third parties.

---

[218] *See supra* notes 192–97 and accompanying text.

[219] *See supra* note 119 and accompanying text (asserting that Framers designed Fourth Amendment, in part, to protect First Amendment rights). The *Katz* Court recognized that the First Amendment protects privacy. Katz v. United States, 389 U.S. 347, 350 & n.5 (1967) ("The First Amendment, for example, imposes limitations upon governmental abridgment of 'freedom to associate and privacy in one's associations.'" (quoting NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958))).

[220] *See* Slobogin, *supra* note 202, at 177 (arguing that URLs should be distinguished from other "catalogic" data, such as transactional data, because they are closer to content).

[221] Richards, *supra* note 18, at 440 (asserting that NSL requests for "intellectual records" would require warrant); Solove, *supra* note 15, at 165 (arguing that government requests for information protected by First Amendment would need warrant supported by probable cause); *cf.* Bellia, *supra* note 193, at 1412 (arguing that law enforcement generally must present warrant to gain access to communications if individual has reasonable expectation of privacy).

[222] The standard of "material importance" is drawn from Solove's argument for a higher protection for third-party records. *See* Solove, *supra* note 179, 1164–65 (2002).

Although revision of the third-party doctrine at the federal level is unlikely to occur,[223] such reform would be, in some ways, superior to relying solely on statutory provisions or the First Amendment. First, revising the third-party doctrine would provide wholesale constitutional protection for our confidential communications. Such a jurisprudential shift would overcome the lack of congressional will to reform[224] and limit the potential for future relaxation of statutory protections, like those in the Patriot Act. It would also avoid the need for a statute-by-statute approach to data privacy. Second, revision of the third-party doctrine would have the benefit of extending collateral protection to First Amendment activities without putting pressure on the First Amendment itself.[225] Reliance on the First Amendment to check government information gathering creates the risk that the deferential Fourth Amendment approach will be transplanted to the First Amendment context, diluting the First Amendment's traditionally more exacting standard of review.[226] Instead, the inverse course could inject some of the First Amendment's strength back into the Fourth Amendment.

Conclusion

To protect national security from the threat of terrorist activity, the government need not sacrifice privacy altogether. The Internet has become an increasingly important means of conducting affairs, from financial transactions to communication. Because third parties such as ISPs hold a blueprint of an individual's online activities, government information gathering through NSLs has the potential to expose major facets of citizens' private lives to scrutiny.

Since the Fourth Amendment currently provides limited protection of data held by third parties, the First Amendment has gained attention as a possible safeguard of online privacy interests. This Note

---

223 *See supra* note 195 and accompanying text; *see also* Henderson, *supra* note 203, at 373 (describing third-party doctrine as having "withstood sustained and even bitter critiques").

224 *See* Slobogin, *supra* note 202, at 188–89 (arguing that constitutional reform is superior because Congress to date has not provided clear and robust safeguards).

225 The D.C. Circuit has noted the potential problem of allowing the First Amendment to protect privacy in criminal investigations, a role already filled by the Fourth and Fifth Amendments. Reporters Comm. for Freedom of the Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1054 (D.C. Cir. 1978).

226 In *Doe IV*, for example, the protection of judicial review under the "reciprocal notice procedure" arguably provides less protection than the Court required in *Freedman v. Maryland*, 380 U.S. 51 (1965). John Doe, Inc. v. Mukasey (*Doe IV*), 549 F.3d 861, 879 (2d Cir. 2008). *See supra* notes 100–01, 111 and accompanying text. Leaving the burden of requesting review with the ISP potentially effected a dilution of First Amendment doctrine.

has argued, however, that the protection of privacy should not rest solely on the First Amendment. Although *Doe IV* provides some protection by subjecting the Patriot Act's nondisclosure requirement to a more robust judicial review process,[227] individual subscribers still have limited protection against NSL requests. Enhanced statutory judicial review or reform of the Fourth Amendment third-party doctrine could better ensure that privacy is not unduly infringed, nor speech or association chilled, while simultaneously allowing the government to pursue its legitimate information-gathering activities.

---

[227] *See supra* Part I.C.2.