NOTES

UNSHEATHING A SHARP SWORD: WHY NATIONAL SECURITY LETTERS ARE PERMISSIBLE UNDER THE FOURTH AMENDMENT

Nickolas J. Bohl[*]

[*] J.D. Candidate, Boston University, 2006.

INTRODUCTION

The FBI wants to know what terrorists are looking at on the Internet – or at least people it suspects are terrorists. This Note asks: does the FBI have this power under the Fourth Amendment? While the Southern District of New York Court recently held that the FBI does not possess such authority,[1] this Note concludes that the Fourth Amendment allows broad-ranging governmental inquiries into individual's Internet and telecommunications activities.

The terrorist attacks of 2001 exacerbated the long-standing struggle between national security and personal privacy,[2] immediately tipping the scales in favor of more national security. But now the pendulum is swinging back. In September 2004 in *Doe v. Ashcroft*, the Southern District of New York Court invalidated 18 U.S.C. § 2709,[3] a statute that allowed the FBI to subpoena an individual's Internet and telephone records based on the individual subscriber's suspected terrorist activities.[4] Not surprisingly, this statute was amended as part of the controversial USA PATRIOT Act of 2001 ("PATRIOT Act"),

[1] Doe v. Ashcroft, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004). The Department of Justice has announced its intention to appeal the district court's ruling. Press Release, Department of Justice, Department's Decision to Appeal the National Security Letter Ruling by the District Court in New York (Sept. 30, 2004), http://www.usdoj.gov/opa/pr/2004/September/04_opa_664.htm.

[2] The case for broad executive power in the name of protecting the public interest has been made before:

> A Commission which is without coercive powers, which cannot arrest or amerce or imprison though a crime has been uncovered . . . but can only inquire and report, the propriety of every question in the course of the inquiry being subject to the supervision of the ordinary courts of justice, is likened with denunciatory fervor to the Star Chamber of the Stuarts. Historians may find hyperbole in the sanguinary simile.

Jones v. Sec. & Exch. Comm'n, 298 U.S. 1, 32-33 (1936) (Cardozo, J., dissenting). In contrast, the case for privacy has been put forth by Mr. Justice Brandeis:

> The makers of our Constitution . . . . conferred, as against the Government, the right to be let alone the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

Olmstead v. United States, 277 U.S. 438, 478-79 (1928) (Brandeis, J., dissenting).

[3] (2000 & Supp. 2002), *invalidated by Doe*, 334 F. Supp. 2d 471.

[4] *Doe*, 334 F. Supp. 2d at 475 (holding the statute unconstitutional on both Fourth and First Amendment grounds). Numerous pieces of federal legislation pertaining to NSLs have been introduced since the invalidation of § 2709, but none have been approved by Congress. *See, e.g.*, S. 2271, 109th Cong. (2006) (clarifying that individuals who receive NSL orders can challenge nondisclosure requirements); S. 1680, 109th Cong. (2005) (reforming the issuance of NSLs).

which broadened government power to fight terrorism.[5] Under § 2709, the FBI can send a National Security Letter (NSL) demanding that telecommunications companies turn over information on the phone or internet activities of suspected terrorists.[6] These letters are considered equivalent to administrative subpoenas, a powerful government tool that usually receives broad protection under the law.[7] Therefore, any evaluation of an NSL must begin with the well-developed doctrines that govern administrative subpoenas.[8]

The district court in *Doe* feared that any compliance with the NSL would be coerced because neither the statute nor the NSL itself explicitly provided for judicial review; therefore the court held that § 2709 permitted an unreasonable search and seizure in violation of the Fourth Amendment.[9] This weighty decision gives telecommunications companies a broad shield to protect against the powerful NSL, a sharp sword that grants the federal government sweeping access to information in the name of combating terrorism Questions about national security and personal privacy are exceedingly complicated. It is imperative not only for Congress to draft thoughtful law, but for courts to review it thoughtfully. There is more at stake than securing political or jurisdictional clout.

This Note explores the legality of § 2709, specifically focusing on its Fourth Amendment implications. Part I briefly examines the background of § 2709, as well as the *Doe* court's reasons for invalidating it. Part II begins the analysis by asking, as a threshold matter, whether an NSL intrudes sufficiently on privacy interests to implicate the Fourth Amendment at all. After considering the general "legitimate expectation of privacy" test and the "assumption of risk" doctrine, this Part concludes that the target of an NSL most likely cannot assert any Fourth Amendment privacy rights in his or her telecommunications records. The conundrum here, however, is whether a telecommunications provider can assert greater rights than the individual subscriber-target; not only is the latter generally more concerned about records remaining private, but he or she is also the actual target of the government's investigation. Part II reaches the seemingly incongruous conclusion that,

[5] *Doe*, 334 F. Supp. 2d at 483.

[6] 18 U.S.C. § 2709.

[7] *See Doe*, 334 F. Supp. 2d at 475 (describing the NSL as a "unique form of administrative subpoena cloaked in secrecy and pertaining to national security interests"); ACLU v. U.S. Dep't of Justice, 265 F. Supp. 2d 20, 29 (D.D.C. 2003) (describing an NSL as an "administrative subpoenas used by the FBI to obtain various kinds of records"); *see also* United States v. Miller, 425 U.S. 435, 446 n.8 (1976) (finding that subpoenas do not have to meet the heightened standards of search warrants); *infra* text accompanying notes 164-167.

[8] *See infra* Part III.A.

[9] *Doe*, 334 F. Supp. 2d at 475 ("The Court concludes that § 2709 violates the Fourth Amendment because, at least as currently applied, it effectively bars or substantially deters any judicial challenge to the propriety of an NSL request.").

under current Supreme Court precedent, the telecommunications company actually has greater privacy interests than the subscriber-target. Based on the assumption that a telecommunications company has a reasonable expectation of privacy in the records, Part III considers whether an NSL constitutes a reasonable search as an administrative subpoena, and whether an NSL coerces compliance. Part III concludes that an NSL, or at least one similar to that in *Doe*, satisfies the minimal administrative subpoena standards and is not coercive. Although the *Doe* court was primarily concerned that neither the statute nor the NSL provided for judicial review, the Supreme Court's precedent makes such an explicit provision unnecessary. The Note concludes that the FBI has the power to compel telecommunications companies to produce records involving suspected terrorists upon only self-certification that the subscriber-target is a suspected terrorist and irrespective of whether the subscriber or the company desires the records to remain private.

I. *DOE V. ASHCROFT*

Section 2709 authorizes the FBI to compel telecommunications companies – either telephone or Internet Service Providers ("ISPs") – to produce customer records.[10] Under § 2709, the FBI must first certify that the records are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities" before they can compel anyone to produce any records.[11]

A. *Legislative History*

Section 2709 was not born out of the PATRIOT Act, only broadened by it.[12] Ironically, Congress actually enacted § 2709 as part of the Electronic Communications Privacy Act of 1986 (E.C.P.A.).[13] The E.C.P.A. was part of a legislative reaction to a series of U.S. Supreme Court cases that, according to Congress, eroded privacy in individuals' records.[14] Through this early form of the legislation, Congress provided bank customers with more Fourth Amendment protection against government investigation by requiring that federal agencies follow certain procedures before accessing or intercepting

[10] 18 U.S.C. § 2709 (2000 & Supp. 2002) ("A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.").

[11] *Id.*

[12] *Doe*, 334 F. Supp. 2d at 480-83 (describing the legislative history of § 2709).

[13] 18 U.S.C. § 2510-22 (2000). This law was codified in part because of Congress' concerns about the dangers of ubiquitous video and electronic surveillance in our society. *See Doe*, 334 F. Supp. 2d at 480-81.

[14] *See Doe*, 334 F. Supp. 2d at 480-81.

electronic communications.[15] Section 2709 has always allowed the FBI to request records upon "a mere self-certification."[16] But prior to the PATRIOT Act amendment of § 2709, the requested information also had to be "relevant to an authorized foreign counterintelligence investigation"[17] and justified by the FBI through "specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power."[18]

Over time, Congress relaxed these restrictions. In 1993, Congress first weakened the requirement that the investigation be attached to a foreign power.[19] Then, the PATRIOT Act entirely replaced the nexus to a foreign power requirement with the current standard, which only requires the target to be associated with an investigation into "international terrorism or clandestine intelligence activities."[20] In general, Congress felt that this would "harmonize[] [§ 2709] with existing criminal law where an Assistant United States Attorney may issue a grand jury subpoena for all such records in a criminal case"[21] and allow the FBI to obtain the information it needed more quickly.[22] This statute, in its amended form, was the subject of contention in *Doe v. Ashcroft*.

---

[15] *Id.* Congress modeled the E.C.P.A. on the Right to Financial Privacy Act (R.F.P.A.) of 1978, which was a direct response to the Court's holding in *United States v. Miller*, 425 U.S. 435 (1976). *See Doe*, 334 F. Supp. 2d at 480-81; *infra* Part II.A.3. Specifically, the R.F.P.A. was "intended to protect the customers of financial institutions from unwarranted intrusion into their records while at the same time permitting legitimate law enforcement activity." H.R. REP. NO. 95-1383, at 33 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 9273, 9305.

[16] *Doe*, 334 F. Supp. 2d at 481.

[17] *Id.* at 482 n.36 (quoting 18 U.S.C. § 2709(b) (1994)).

[18] *Id.* The original stricter standards were designed to ensure compliance with the First and Fourth Amendments. *Id.* at 482 (referring to Congressional comments about the statute).

[19] H.R. REP. NO. 103-46, at 2 (1993), as *reprinted in* 1993 U.S.C.C.A.N. 1913, 1914-15 (recognizing that Congress had enlarged the purview of the NSL, but concluding that the change was necessary for the FBI to accomplish its goals).

[20] 18 U.S.C. § 2709 (2000 & Supp. 2002). The *Doe* court noted that one of Congress' reasons for increasing the FBI's power was an episode where the FBI had insufficient authority to track down a possible national security threat. *Doe*, 334 F. Supp. 2d at 483 n.37. The FBI had intercepted a phone call from an unidentified federal employee offering to provide sensitive intelligence information to a foreign nation. *Id.* According to the FBI, the original version of § 2709 did not permit it to trace the employee's call because the employee was a possible volunteer as a foreign agent, and not himself a foreign agent. *Id.* Therefore, the FBI could not identify him. *Id.*

[21] H.R. REP. NO. 107-236, at 62 (2001) (discussing the 2001 amendments to § 2709).

[22] *Doe*, 334 F. Supp. 2d at 483.

B. *District Court Decision in* Doe v. Ashcroft

John Doe, an unnamed ISP, received an NSL on FBI letterhead.[23] This letter: (i) "directed" him to provide information to the government; (ii) "certified" that the information would be relevant to an authorized terrorist investigation; and (iii) "advised" him that he was prohibited from disclosing to any person that the FBI sought or obtained these records.[24] Instead of complying, Doe, along with the American Civil Liberties Union, sued the Attorney General and the FBI, challenging the constitutionality of § 2709.[25] The *Doe* court wrote a 122-page opinion that found in favor of Doe and invalidated § 2709 on both First and Fourth Amendment grounds.[26] This Note explores only the *Doe* court's Fourth Amendment arguments. The district court's analysis was incomplete; it neither addressed the full spectrum of issues, such as why Doe had any Fourth Amendment interests in the requested material, nor examined the full complement of Second Circuit precedent to determine whether Doe was actually coerced.

The *Doe* court began its discussion by clarifying that the Fourth Amendment rights at issue were those of the ISP, and *not* the target of the FBI's investigation.[27] The court determined that the target had very limited privacy interests in the information he had voluntarily conveyed and exposed to a third party (Doe, his ISP).[28] Under the court's analysis, Doe had seemingly greater privacy rights than the target because Doe had not exposed the records and was contractually obligated to protect the anonymity of its client.[29] Within this context, the court examined the reasonableness of the NSL as an administrative subpoena.[30]

The *Doe* court carefully evaluated the subpoena process and compared the language of § 2709 to other statutes authorizing NSLs and administrative

[23] *Id*. at 478.

[24] *Id.* at 478-79 (observing that Doe also had several conversations with the same FBI agent before contacting A.C.L.U. attorneys).

[25] *Id.* at 479 (specifying that Doe never did comply with the NSL request).

[26] *Id.* at 525-27. Specifically, the court held that the statute violated the First and Fourth Amendments, and also that § 2709(c) was not narrowly tailored enough to advance the compelling government interest of protecting national security in terrorism investigations. *Id.*

[27] *Id.* at 494 n.118 ("To be clear, the 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.").

[28] *Id.* ("Individuals possess a limited Fourth Amendment interest in records which they voluntarily convey to a third party.")

[29] *See id.* (finding that "many potential NSL recipients may have particular interests in resisting an NSL, e.g., because they have contractually obligated themselves to protect the anonymity of their subscribers . . . .").

[30] *Id.* at 495.

subpoenas.[31] Most alarming to the court was that § 2709 did not specifically allow for judicial review of the NSL.[32] The court rejected the government's argument that a lack of judicial review was mere oversight and otherwise implied by the law.[33] According to the *Doe* court, a permissible reading of the legislative history is that Congress wanted the FBI to have greater authority under § 2709 than under other administrative subpoena statutes, without having to worry about judicial meddling.[34]

The lack of judicial review concerned the *Doe* court for two reasons.[35] First, it was not clear that an NSL recipient could consult an attorney about the NSL without violating § 2709's non-disclosure provision.[36] Second, the statute contained neither an explicit provision for judicial enforcement of an NSL against a recipient who refused to comply, nor one that allowed a recipient to challenge the propriety of an NSL request.[37] Therefore, even if Doe believed that the records were not relevant to international terrorism, it could not seek judicial review of the NSL or even discuss its concerns with anyone. The *Doe*

[31] *Id.* at 484-87, 491-93. Three of the statutes provided a framework for the issuance of NSLs in other contexts. *See* 12 U.S.C. § 3414 (2000 & Supp. 2004) (financial records); 15 U.S.C. § 1681u (2000) (credit records); 15 U.S.C. § 1681v (2000 & Supp. 2002) (credit records); 50 U.S.C. § 436 (2000) (government employee records). Four of the statutes dealt with administrative subpoenas in general. *See* 7 U.S.C. § 4610a(b) (2000) (granting the Secretary of Agriculture power to issue subpoenas to investigate and enforce laws related to honey research); 15 U.S.C. § 78u(b) (2000) (granting the SEC power to issue subpoenas to investigate possible violations of the securities laws); 16 U.S.C. § 773i(f)(2) (2000) (codifying the Secretary of Commerce's power to issue subpoenas to investigate and enforce halibut fishing laws); 26 U.S.C. § 7602(a) (2000) (setting out the IRS's power to issue subpoenas to investigate possible violations of the tax code). As discussed *infra* in Part III.C.1, there are few differences between other NSL statutes and § 2709, which potentially broadens the scope of the opinion.

[32] *Doe*, 334 F. Supp. 2d at 475 (concluding that "§ 2709 violates the Fourth Amendment because . . . it effectively bars or substantially deters any judicial challenge to the propriety of an NSL request").

[33] *Id.* at 496-506.

[34] *Id.* at 500 (arguing that "one might fairly infer that the absence of any reference to judicial review is the product of Congressional intent").

[35] *Id.* at 492.

[36] *Id.* at 502 ("Because neither the statute, nor an NSL, nor the FBI agents dealing with the recipient say as much, all but the most mettlesome and undaunted NSL recipients would consider themselves effectively barred from consulting an attorney or anyone else who might advise them otherwise"); *see also* 18 U.S.C. § 2709(c) (2000 & Supp. 2002) (forbidding the recipient, officer, employee, or agent to disclose any information about the NSL).

[37] *Doe*, 334 F. Supp. 2d at 501 (emphasizing the lack of "access to legal advice and availability of judicial process to enforce and contest the law" as the core deficiencies in § 2709). Of the administrative subpoena statutes that the court compared to § 2709, only 15 U.S.C. § 1681u specifically codifies a penalty for noncompliance. *See* 15 U.S.C. § 1681u(j) (2000 & Supp. 2002).

court examined the legislative history and found that Congress recognized these problems, and that some Representatives had even introduced legislation to cure these deficiencies.[38] Based on these findings, the court concluded that Congress may have intentionally denied a right to judicial review, thereby giving the FBI expansive power to investigate; the court further concluded that such power violated the Fourth Amendment.[39] According to the court, without these necessary judicial safeguards neither the NSL recipient nor the target of the FBI's investigation could challenge the FBI's violations of their respective Fourth Amendment rights.[40]

The government tried to persuade the *Doe* court that it had misconstrued the statute's language.[41] Initially, the government acknowledged a sharp distinction between agency power to issue subpoenas and judicial power to enforce them, agreeing that the former cannot exist without the latter.[42] Nevertheless, the government claimed that the statute implicitly allowed someone to challenge an NSL, considering such an interpretation is built into many administrative subpoena statutes.[43] The reasoning was that because a corporation must act through its agents, Doe, as an agent of the corporation, would naturally be allowed to contact his attorneys.[44] Indeed, the government argued, a minimal amount of disclosure was necessary for essential employees to comply with the subpoena.[45] It would be unreasonable for an individual NSL recipient to do all the work herself, especially in a large

[38] *Doe*, 334 F. Supp. 2d at 492 & n.110 (citing a proposed Congressional bill to amend § 2709 to allow the FBI to seek judicial enforcement). *See* H.R. 3179, 108th Cong. (2004); *The Anti-Terrorism Intelligence Tools Improvement Act of 2003: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 108th Cong. (2004) (opening statement of Rep. Coble, Chairman, Subcommittee on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary):

> The current law authorizes the Federal Government to use a National Security Letter, which is basically an administrative subpoena, to make a request for transactional records, such as billing records. These requests must be related to investigations of international terrorism or clandestine intelligence activities. The current law, however, has no mechanism to enforce the requests. Furthermore, the current law provides no penalty for an individual who decides to tip off a target of a terrorism or an intelligence investigation that the Federal government has made a National Security letter request concerning the target.

[39] *Doe*, 334 F. Supp. 2d at 500.

[40] *Id.* at 506 (finding that "§ 2709, as applied here, must be invalidated because in all but the exceptional case it has the effect of authorizing coercive searches effectively immune from any judicial process, in violation of the Fourth Amendment").

[41] *Id.* at 496-97.

[42] *Id.* at 497.

[43] *Id.* at 497-98 (pointing to the legislative history of § 2709).

[44] *Id.* at 497.

[45] *Id.*

telecommunications corporation.[46] The *Doe* court acknowledged that these arguments were apposite, but their merit was outweighed by the court's concerns about § 2709's usurpation of judicial authority.[47]

Though the *Doe* court recognized it should uphold the legislation if any permissible construction so allowed,[48] it found that no reading could repair the practically coercive power of the NSL.[49] Rather than looking at the words used in the statute, the court found the "sounds of silence" in the statute dispositive.[50] According to the *Doe* court, the absence of a judicial review provision suggested that Congress succumbed to the grave national security concerns of the day and specifically intended to deprive NSL recipients of such recourse.[51] The "crux of the problem," in the court's eyes, was that the NSL fatally combined secrecy and coercion.[52] The *Doe* court feared that without its intervention NSL's would continue to allow unchecked government power because the language and tone of the letter would coerce any recipient into complying.[53] Therefore, the *Doe* court held that the NSL's coercive tone, aggravated by a perceived lack of judicial review, violated Doe's Fourth Amendment rights.[54]

In determining whether an NSL violates the Fourth Amendment, this Note divides the analysis into two questions. The first examines whether the NSL rises to the level of a search or seizure protectable under the Fourth

[46] *Id.* The government relied on two Second and Sixth Circuit cases that allowed parties sworn to secrecy to communicate with their attorneys. *Id.* at 498 & n.136 (citing Nix v. O'Malley, 160 F.3d 343, 351 (6th Cir. 1998) (holding that "the defendant may disclose to his attorneys the contents of intercepted communications"), and McQuade v. Michael Gassner Mech. & Elec. Contractors, Inc., 587 F. Supp. 1183, 1190 (D. Conn. 1984) (finding that defendant's counsel can listen to intercepted communications and recordings to prepare a defense)).

[47] *Id.* at 505-06.

[48] *Id.* at 498.

[49] *Id.* at 506 (concluding that "what is, in practice, an implicit obligation of automatic compliance with NSLs violates the Fourth Amendment right to judicial access, even if hypothetically the law were construed to imply such access").

[50] *Id.* at 499 & n.141 (quoting SIMON & GARFUNKEL, SOUNDS OF SILENCE (Columbia Records 1966)).

[51] *Id.* at 492-94.

[52] *Id.* at 501:

> The crux of the problem is that the form NSL, . . . which is preceded by a personal call from an FBI agent, is framed in imposing language on FBI letterhead and which, citing the authorizing statute, orders a combination of disclosure *in person* and in complete secrecy, essentially coerces the reasonable recipient into immediate compliance.

[53] *Id.* at 501-03 (dismissing the government's argument that because the very fact that Doe consulted an attorney and brought this case showed that a reasonable person would feel comfortable doing so and, further, finding persuasive the fact that the government had never needed to seek judicial enforcement of an NSL).

[54] *Id.* The court noted in particular that "evidence suggests that perhaps even the FBI does not actually believe that § 2709 contemplates judicial review." *Id.* at 502 n.146.

Amendment; assuming that it does, the second part explores whether that search or seizure is reasonable.

II. IS A NATIONAL SECURITY LETTER A SEARCH OR SEIZURE?

Fourth Amendment law is a thorny muddle of complex, sometimes contradictory law. Reaching the correct conclusion – one that best comports with precedent – requires both careful and thorough analysis. Such analysis was lacking in the *Doe* court decision.

The *Doe* court's analysis focused on the NSL's reasonableness.[55] While certainly crucial, this is not the whole issue. Fourth Amendment jurisprudence demands a dual inquiry. First, a court must determine whether there has been a "search" or "seizure" within the meaning of the Fourth Amendment.[56] In order to find either of these protected concepts, the government action must be found to invade a reasonable privacy interest.[57] Second, if the intrusion reaches the level of a search or seizure, then the court must determine if that intrusion itself was reasonable.[58] This reasonableness evaluation balances the government's need for the information against the individual's privacy and possessory interests.[59]

The factual setting of Doe's case complicates the analysis. There are two distinct parties with potential Fourth Amendment claims: the target of the FBI's investigation and the company itself, Doe.[60] Therefore, we must examine, as discrete questions, whether either the target or Doe had any protected interest in the subpoenaed information. If the target has no Fourth Amendment rights in the records' privacy, then we must determine whether Doe's possessory and property interests are greater than the target's privacy interest.[61] The issue is further complicated because the NSL is considered to

[55] *Id.* at 495-96.

[56] *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection [i.e., is not a "search"].").

[57] *See id.* at 352 (finding that one who occupied a telephone booth, shut the door, and paid to use the public telephone had a reasonable expectation of privacy).

[58] *See* New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) ("Although the underlying command of the Fourth Amendment is always that searches and seizures be reasonable, what is reasonable depends on the context within which a search takes place.").

[59] Michigan v. Sitz, 496 U.S. 444, 449-50 (1990) ("Where a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context." (quoting Treasury Employees v. Von Raab, 489 U.S. 656, 665-66 (1989))). The government has a special need beyond that of normal law enforcement to investigate and root out terrorist operations in the United States.

[60] *See supra* notes 27-28 and accompanying text.

[61] These competing rights between Doe and the target raise a potential standing concern. The Supreme Court's standing jurisprudence changed significantly after the landmark cases

be an administrative subpoena and therefore imports its own body of law, which will be analyzed in Part III.

The *Doe* court did not thoroughly analyze whether the target had any Fourth Amendment rights and all but presumed Doe's Fourth Amendment rights were implicated; instead, most of the opinion focuses on the reasonableness of the intrusion.[62] The court buried its brief analysis of the threshold issue, of whether a search or seizure had occurred, within a footnote.[63] Instead, the *Doe* court found an invasion of Doe's privacy because "many potential NSL recipients may have particular interests in resisting an NSL, e.g., because they have contractually obligated themselves to protect the anonymity of their subscribers, or because their own rights are uniquely implicated by what they regard as an intrusive and secretive NSL regime."[64] This loaded footnote accepts that the target likely has no expectation of privacy and implies that Doe has greater interests.[65] But the only support the court musters for this somewhat surprising claim is the anonymity Doe contractually promised and Doe's "uniquely implicated" rights, without expounding on what those may be.[66]

Therefore, this Note first seeks to do what the *Doe* court did not: determine whether the NSL implicates either the target's or Doe's Fourth Amendment interests.

A. *Definitions and Doctrines*

1. Seizure

Before determining whether the government's conduct in *Doe* actually qualifies as a search or seizure, it is necessary to understand what these terms

Rawlings v. Kentucky, 448 U.S. 98, 105-06 (1980) (holding that the defendant did not have standing to challenge the search of his companion's purse because he had no reasonable expectation of privacy in her purse despite his possesory interest in the drugs that he had placed there), and *Rakas v. Illinois*, 439 U.S. 128, 143 (1978) (separating a violation of a person's Fourth Amendment rights from a trespass violation of his property). The current approach subsumes the standing issue into the threshold inquiry of whether the defendant had a legitimate expectation of privacy in the area searched. *See Rakas*, 439 U.S. at 139. *Rawlings* went even further to hold that a defendant has no standing if he has no legitimate expectation of privacy in the area searched, even if he had a possessory or ownership interest in the property seized. *Rawlings*, 448 U.S. at 105-06. Therefore, both Doe and the target can press only their own privacy interests.

[62] Doe v. Ashcroft, 334 F. Supp. 2d 471, 476 (S.D.N.Y. 2004) ("The Court decides only that [the Fourth Amendment] rights . . . are implicated to *some* extent when an individual receives an NSL . . . .") (emphasis added).

[63] *Id.* at 494 n.118.

[64] *Id.*

[65] *See id.*

[66] *Id.*

mean in the Fourth Amendment context.[67] A "seizure" is usually defined either as an "act of physically taking and removing tangible personal property"[68] or "meaningful interference with an individual's possessory interests in that property."[69] Applying this definition to the *Doe* case, it is clear that no Fourth Amendment seizure has occurred against the target. Because the target was not in possession of the records, the government could neither physically remove them from the target's control nor interfere with the target's possessory interest.[70]

Nevertheless, the NSL might constitute a seizure against Doe. And while the government is asking for Doe's property, it is not Doe's *personal* property. The remaining question, therefore, is whether there was a meaningful interference by the government with Doe's possessory interest in the target's records. This issue will be explored below as part of the impermissible search analysis, which considers whether the government meaningfully interfered with Doe's reasonable expectation of privacy.[71]

2. Search and the Reasonable Expectation of Privacy

The Supreme Court has been reluctant to give a comprehensive definition of "search"[72] and has been careful to note that every act of government investigation is not necessarily a search under the Fourth Amendment.[73] The Supreme Court significantly broadened its Fourth Amendment jurisprudence by introducing the issue of a defendant's reasonable expectations of privacy into search and seizure analysis.[74] In 1967, the landmark decision *Katz v. United States* held that for a defendant to receive Fourth Amendment protection a court must decide if the defendant had a reasonable expectation of

[67] *See* WAYNE LAFAVE, SEARCH & SEIZURE § 2.1(a) (3d ed. 1996) (discussing the Supreme Court's evolving understanding of these terms).

[68] *Id.* at 375-76 (quoting 68 AM. JUR. 2D *Searches and Seizures* § 8 (1973)).

[69] United States v. Jacobsen, 466 U.S. 109, 113 (1984) (finding "meaningful interference" when government agents exerted dominion and control over a package that had been in the possession of a private freight carrier). *But see* United States v. Karo, 468 U.S. 705, 712-13 (1984) (finding no such meaningful interference when government agents installed a tracking device on defendant's property).

[70] *See Doe*, 334 F. Supp. 2d at 494 n.118.

[71] *See* discussion *infra* Part II.C.

[72] LAFAVE, *supra* note 67, § 2.1(a), at 379-80 (stating that a search is generally "some exploratory investigation, or an invasion and quest, a looking for or seeking out" (quoting C.J.S. *Searches and Seizures* § 1 (1952))).

[73] *See* Coolidge v. New Hampshire, 403 U.S. 443, 489-90 (1971) (finding no search or seizure when, in response to the police's inquiry whether there were guns in the house, defendant's wife voluntarily turned over his guns).

[74] Katz v. United States, 389 U.S. 347, 351-52 (1967) (rejecting the previous trespass-based approach, which required a physical intrusion into a constitutionally protected area); *see also* Silverman v. United States, 365 U.S. 505, 510-12 (1961) (questioning the trespass doctrine, which was later overturned in *Katz*).

privacy in the implicated activity.[75] To answer this daunting question, Justice Harlan's concurrence created a two-prong test: first, a person must exhibit a subjective expectation of privacy, and, second, this expectation must be one that is objectively "reasonable" to society.[76]

a. *Subjective Prong*

The subjective prong of the analysis asks whether the defendant personally expected his or her activities to remain private.[77] But some courts have rejected any suggestion that *Katz* demands an actual, subjective expectation of privacy.[78] Most defendants, acting in their own best interests, would likely argue that they had an expectation of privacy in the seized material. One's subjective belief is difficult to disprove, which significantly limits the dispositive power of the subjective prong.[79] The defendant's Fourth Amendment rights may be curtailed if the government can show the defendant could not subjectively expect his actions to remain private,[80] and the absence of any subjective intention may hurt the suspect's case.[81] In application, the Court has demanded that a person take steps to ensure his or her privacy

[75] *Katz*, 389 U.S. at 351-52 ("[T]the Fourth Amendment protects people, not places. . . . [W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

[76] *Id.* at 361-62 (Harlan, J., concurring) (explaining that while a person's home may be a place where that person reasonably expects privacy, acts done in "plain view" of the public do not carry the same expectation).

[77] *Id.*; LAFAVE, *supra* note 6754, § 2.1(c).

[78] *See* United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) ("The analysis must, in my view, transcend the search for subjective expectations or legal attribution of assumptions of risk. Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present."); United States v. Taborda, 635 F.2d 131, 137 (2d Cir. 1980) (rejecting a purely subjective prong); *see also* Eric Dean Bender, Note, *The Fourth Amendment in the Age of Aerial Surveillance: Curtains for the Curtilage?*, 60 N.Y.U. L. REV. 725, 743-45 (1985) (detailing the types of subjective analysis that occur in curtilage cases).

[79] *See* California v. Ciraolo, 476 U.S. 207, 211-15 (1986) (acknowledging that "respondent ha[d] met the test of manifesting his own subjective intent and desire to maintain privacy as to his unlawful . . . pursuits," but nevertheless finding no Fourth Amendment violation).

[80] *See* United States v. Miller, 425 U.S. 435, 442 (1976) (perceiving no "expectation of privacy" in the contents of defendant's original checks and deposit slips); *see also infra* Part III.A.2.b.

[81] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited.").

against almost all government scrutiny.[82] Yet other decisions suggest that this mandate is fulfilled as long as one demonstrates an intention to maintain privacy and not "knowingly expose" one's property "to the open view of the public."[83] Although courts have created confusion by applying these various standards, at the very least, the defendant must exhibit some intent to keep his or her activities secret.

b. *Objective Prong*

The subjective prong is of limited importance to the Supreme Court.[84] The central part of the analysis, and perhaps the only relevant part, is determining whether society is prepared to recognize the defendant's privacy interest as reasonable.[85]

This determination is a difficult one.[86] The Court has endeavored to create a test that is based primarily on the Fourth Amendment's core values and is detached from precedent.[87] Justice Harlan asserted that courts must determine what is reasonable by "assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement."[88] Therefore, courts must define the defendant's appropriate sense of security, ascertain how important it is, and decide if government activities invade that sense of security. When evaluating this sense of security, the Supreme Court instructs courts to look "at the customs and values of the past and present,"[89] and to assess the harm of any government invasion by considering the effect of allowing the government to regularly engage in such conduct, limited only by

[82] *See Ciraolo*, 476 U.S. at 213 ("Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible.").

[83] Bender, *supra* note 78, at 754.

[84] LAFAVE, *supra* note 67, § 2.1(c).

[85] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("The [Fourth]Amendment does not protect the merely subjective expectation of privacy, but only those expectation[s] that society is prepared to recognize as reasonable.") (internal quotation marks and citation omitted).

[86] *See* LAFAVE, *supra* note 67, § 2.1(d).

[87] *See* Edmund W. Kitch, Katz v. United States*: The Limits of the Fourth Amendment*, 1968 SUP. CT. REV. 133, 133 (1968) (comparing the Supreme Court's Fourth and Fifth Amendment analyses).

[88] United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting). While Harlan's dissent is not controlling precedent, his explanation on reasonability is persuasive, considering the Court's later reliance on his *Katz* concurrence.

[89] *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974) (contemplating how much and what type of government surveillance should be permitted by courts).

its self-restraint.[90] The question is essentially whether allowing this particular government conduct requires society to give up too much freedom.[91] This calls for courts to think abstractly about the relevant activities. Courts assess the reasonability of the search or seizure itself by scrutinizing the particular facts and circumstances.[92]

3. Assumption of Risk

These subjective and objective expectations can be considerably altered when the defendant exposes potential evidence to the world. When *Katz* held that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection,"[93] the Court gave birth to an "assumption of risk" analysis that significantly colors the outcome in *Doe*.[94] Generally, if one assumes the risk of exposing contraband to any third party, one also assumes the risk of exposing it to law enforcement and thus losing any Fourth Amendment protection. [95] Although the *Doe* court tried to distance itself from this type of analysis,[96] the Supreme Court has continued to reaffirm and even strengthen this idea.[97] Three pertinent cases show the vitality of the assumption of risk analysis: *United States v. Miller*,[98] *Smith v. Maryland*,[99] and *California v. Greenwood*.[100] These are not the only cases applying the assumption of risk analysis, but they have the most application to the *Doe* fact pattern.

In 1976, the Supreme Court sounded a victory for law enforcement and a defeat for anyone with bank records.[101] In *United States v. Miller*, the Court

[90] *Id.*:

> The ultimate question . . . is whether, if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society.

[91] *Id.*

[92] *See infra* Part III for this analysis.

[93] Katz v. United States, 389 U.S. 347, 351 (1967).

[94] *See* LAFAVE, *supra* note 67, § 2.4(b).

[95] *Id.* This assumption of risk analysis is similar to the plain view doctrine, which states that officers may seize an item without a warrant if it is in "plain view." In particular, an item in plain view may be seized if: (1) the officer is lawfully on the scene; (2) the officer has a right of access to it; and (3) the officer has probable cause to believe that the object is contraband. *See* Horton v. California, 496 U.S. 128, 136-37 (1990); Arizona v. Hicks, 480 U.S. 321, 326 (1987); Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971); *see generally* LAFAVE, *supra* note 67, § 2.2(a).

[96] *See supra* notes 27-30 and accompanying text.

[97] LAFAVE, *supra* note 67, § 2.1(b).

[98] 425 U.S. 435 (1976).

[99] 442 U.S. 735 (1979).

[100] 486 U.S. 35 (1988).

[101] *Miller*, 425 U.S. at 445.

held that the defendant "had no protectable Fourth Amendment interest in the subpoenaed [bank] documents" because the records had already been exposed to a third party, the bank.[102] *Miller* triggered a quick legislative reaction.[103] Congress was concerned that the breadth of police power could intrude into the sanctuary of people's finances and, in reaction, passed the Right to Financial Privacy Act.[104] This Act significantly eroded the specific holding of *Miller*, as it relates to bank records, by putting in place particular procedures law enforcement must follow. Nevertheless, the assumption of risk analysis is still good law; courts continue to apply the doctrine and ask whether the defendant assumed the risk of law enforcement discovering the illicit material.[105]

Like *Doe*, *Smith v. Maryland* involved the telecommunications industry.[106] The Court held that Smith had no legitimate expectation of privacy in telephone numbers he dialed because he "knowingly" conveyed them to a third party, the telephone company.[107] This principle seems directly applicable to the target in *Doe*, where the target has knowingly conveyed his internet information to the ISP, Doe.

The Supreme Court broadened the assumption of risk analysis in *California v. Greenwood*, holding that a person does not have a legitimate expectation of privacy in his own garbage.[108] The Court reasoned that when Greenwood put his garbage on his curb, he assumed the risk that any person would rifle through it. As discussed below, these cases alter both prongs of the *Katz* test

[102] *Id*. at 437. The Bureau of Alcohol, Tobacco, and Firearms had issued subpoenas to Miller's bank while investigating charges of possessing an unregistered still, operating a distillery without bond or paying whiskey taxes, and possessing untaxed whiskey. *Id.* at 437, 440. Miller was successful in the lower courts because those courts relied on *Boyd v. United States*, 116 U.S. 616, 622-23 (1886), *abrogated by* Fisher v. United States, 435 U.S. 391 (1971). *See Miller*, 425 U.S. at 439. However, the Court disregarded any reliance on *Boyd* on the ground that "the documents subpoenaed here are not the respondent's 'private papers.'" *Id.* at 440.

[103] LAFAVE, *supra* note 67, § 2.7(c).

[104] 12 U.S.C. §§ 3401-3422 (2000) (defining financial record as "any record held by a financial institution pertaining to a customer's relationship with the financial institution"). In *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 745 (1984), the Court discusses the congressional response to the *Miller* holding as an attempt to balance the interests of depositors and banks against those of government agencies.

[105] *See* Kyllo v. United States, 533 U.S. 27, 35 (2001) (finding that a homeowner did not assume the risk of law enforcement being able to use thermal imaging to look through the walls of his house).

[106] 442 U.S. 735 (1979). In *Smith*, the victim of a robbery received telephone calls from a person claiming to be the robber. *Id.* at 737. The police installed a pen register at the central telephone station without an order. This allowed the police to trace the number from which the alleged robber, Smith, called. *Id.* He was soon after arrested, but argued that the pen register illegally seized his number and constituted an illegal search. *Id*.

[107] *Id*. at 742.

[108] 486 U.S. 35, 40-41 (1988).

anytime a defendant exposes contraband to a third party by sharply limiting Fourth Amendment protection in such circumstances.

a. *Subjective Prong*

The first prong of the *Katz* test is significantly diminished under the Supreme Court's assumption of risk analysis. In *Miller*, the Court found that any subjective belief by Miller that the bank would maintain his confidence was irrelevant.[109] Similarly in *Smith*, the Court did not rely on Smith's subjective expectations, finding the Fourth Amendment inquiry might be susceptible to mischief if subjective expectations have been conditioned by external influences.[110] Finally, in *Greenwood*, although the Court enumerated numerous indicia of subjective intent,[111] it found Greenwood's subjective expectation of privacy was irrelevant because he had sufficiently exposed his garbage, defeating any Fourth Amendment claim.[112] Therefore, when defendants knowingly expose evidence to the public, they essentially negate any subjective interest they had.

b. *Objective Prong*

The assumption of risk doctrine also alters the analysis of the objective prong of the Fourth Amendment protection test. The *Miller* Court found that a bank customer assumed the risk of exposure to the government merely by "revealing his affairs" to the bank, and that society would not find the expectation of privacy in those affairs to be reasonable.[113] Similarly, in *Smith*, the Court found that a reasonable telephone user must realize that he conveys phone numbers to the telephone companies, and he cannot expect that his

[109] United States v. Miller, 425 U.S. 435, 443-44 (1976):

> The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

[110] *Smith*, 442 U.S. at 740, n.5:

> For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects . . . In such circumstances, where an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a 'legitimate expectation of privacy' existed in such cases, a normative inquiry would be proper.

[111] The Court found the following indicia: the garbage was contained in opaque bags; the defendant expected the garbage to be removed shortly; contraband was commingled with other trash; and there was very little likelihood that one would rifle through his trash or that he would want them to do so. *Greenwood*, 486 U.S. at 39.

[112] *Id.* at 40.

[113] *Miller*, 425 U.S. at 443.

dialed numbers will be secret.[114] Also, in *Greenwood*, no objective expectation of privacy was found to exist after the defendant had exposed his garbage to the public.[115] Any third party had access to Greenwood's trash, as it was "readily accessible to animals, children, scavengers, snoops, and other members of the public."[116] In these cases, the Court affirmed that law enforcement officers cannot reasonably be expected to "shield their eyes" from what could be observed by any member of the public.[117] Therefore, once a defendant has exposed the evidence to third parties, any objective expectation of privacy is generally defeated.

B. *Does a National Security Letter Implicate the Target's Fourth Amendment Rights?*

These doctrines can now be applied, in turn, to both the target of the investigation and Doe to see if either has any Fourth Amendment interests. The crucial question regarding the applicability of the Fourth Amendment to both the target and the ISP, all but ignored by the *Doe* court, must first be addressed before turning to any inquiry into the reasonableness of the NSL as an administrative subpoena. If neither the target nor Doe has any Fourth Amendment rights in the requested material, then any subsequent analysis is moot; there simply is no Fourth Amendment issue.

1. Subjective Prong

Both the target and Doe likely expected the telecommunications records to remain private, but two fundamental barriers limit the target of an NSL from manifesting any subjective interest in privacy. First, the target might have been unaware any documents or records existed.[118] Second, the target never had access to the documents. Therefore, the target could not take any

[114] *Smith*, 442 U.S. at 742-43. Specifically, the Court relied on the fact that a customer receives information from monthly bills regarding phone numbers he has called, as well as a belief that customers are generally aware of telecommunications technology that allows providers to store numbers customers have dialed. *Id.* Also, each telephone book informed subscribers that pin devices could be used to identify and eventually stop unwelcome calls. *Id.*

[115] *Greenwood*, 486 U.S. at 39-41 ("[A subjective] expectation of privacy does not give rise to Fourth Amendment protection, however, unless society is prepared to accept that expectation as objectively reasonable.").

[116] *Id.* at 40 (footnotes omitted).

[117] *See* California v. Ciraolo, 476 U.S. 207, 213 (1986) ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.").

[118] It is difficult to assess the general awareness that the average Internet user has of his or her exposure. At one extreme, the paranoid user fears anyone can see everything; at the other, the confident user "surfs" under the erroneous assumption that their activities are anonymous. The average user is likely in between, expecting some, but not all, information to be exposed.

affirmative conduct and exhibit a subjective expectation of privacy in the records.[119] But the target could argue that the items were not exposed to the public, and therefore any further action on his part would be superfluous. Additionally, most clients assume that a company will take the necessary steps to keep their private information confidential.[120]

Nevertheless, any subjective interest the target had in the information is immaterial because the information was already exposed to the world.[121] By merely using the Internet or telephone, the target revealed this information, defeating any showing that he subjectively expected the information to be kept private. The government does not have to show that the target actually knew the information was exposed, only that he should have known.[122] The *Smith* Court did not need to find that Smith had a sophisticated understanding of telephone company technology to hold that a reasonable person would know such information was being conveyed as a matter of general knowledge.[123] Even if the target hoped the telecommunications records would remain private, the *Miller* Court was not persuaded by such reliance; it only mattered that the defendant knew or should have known the records were exposed.[124] It does not seem likely that the target can exhibit any subjective privacy interest in the records.

2. Objective Prong

The lack of a subjective privacy interest might be inconsequential if the target can convince the court that there is an objectively reasonable expectation that the records would remain private unless the government obtained a warrant.[125] As with his subjective interest, it will be difficult for the target to show any objective privacy interest because the records have been publicly exposed.

---

[119] *See supra* note 81-83 and accompanying text.

[120] This argument led the *Doe* court to find that Doe, as a corporation, had Fourth Amendment interests, although the target did not. *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 494 n.118 (S.D.N.Y. 2004) ("To be clear, the 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.").

[121] *See* Katz v. United States, 389 U.S. 347, 351 (1967); *see also supra* Part II.A.3 (discussing the assumption of risk doctrine).

[122] *See* Smith v. Maryland, 442 U.S. 735, 742-43 (1979).

[123] *Id*. at 742:

> All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.

[124] United States v. Miller, 425 U.S. 435, 443-44 (1976).

[125] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

Despite the hardships in showing an objective privacy interest in records that have been publicly exposed, the customs and values of the past strongly suggest that these records should be protected. One's Internet activity opens a wide door into one's private affairs. Traditionally, the idea of the government having unhampered access to such a wealth of information has been troubling.[126]

The customs and values of the *present*, however, alter this analysis. The heightened threat to national security, brought about by the September 11, 2001, terrorist attacks, has permeated society in numerous ways, and partly eroded reasonable expectations of privacy.[127] Perhaps an NSL only minimally impacts an otherwise strong sense of security in the records. But although Internet records likely possess great utility for law enforcement, this might not be enough to suggest that society would abdicate such a large privacy interest, relying only on the government's internal controls.

Even if the *Katz* analysis suggests that there should be some Fourth Amendment protection, we must still consider the target's interests under the assumption of risk doctrine. The government has to show only that a reasonable person would realize the information he or she conveys would be exposed.[128] Similar to the use of a telephone under the *Smith* analysis, society expects the target to realize his Internet activities are accessible to Doe.[129] One does not need an intimate knowledge of network circuitry to know that an ISP can track information about its customer's habits. Moreover, under *Greenwood*, one does not even need to knowingly expose the evidence.[130] A reasonable person knows the dangers of the omnipresent "computer hacker" threat. The millions of dollars poured into security software, designed to protect people's electronic data from theft, is a testament to the ubiquitous knowledge that the Internet is a dangerous place.

The *Miller* Court qualified its holding that Miller had no reasonable expectation of privacy in his bank records by acknowledging that it was "[n]ot confronted with a situation in which the Government, through 'unreviewed

---

[126] *See* Boyd v. United States, 116 U.S. 616, 625-26 (1886) (discussing "writs of assistance," which gave the British Crown nearly unfettered access even to private homes to search for smuggled goods).

[127] *See* United States v. Mohrmann, 2004 U.S. Dist. LEXIS 8569, at *21 (D. Kan. 2004) (finding that recent terrorist attacks affected the defendant's reasonable expectations of privacy).

[128] *See* Smith v. Maryland, 442 U.S. 735, 742-43 (1979).

[129] One potential difference between a telephone number and an Internet address is that an Internet address generally conveys more information about what the subscriber is doing. Of course, a telephone number can also convey a sense of the caller's conversation if the call is to a particular business. Other than this distinction, the technology between the two is similar. Any number a caller dials must be processed by the telephone company's technology, while any Internet address a subscriber visits must be processed by the ISP's servers.

[130] California v. Greenwood, 486 U.S. 35, 39 (1988).

executive discretion,' has made a wide-ranging inquiry that unnecessarily 'touch[es] upon intimate areas of an individual's personal affairs.'"[131] Therefore, if the target could show the NSL was overreaching, and touched upon intimate areas of his or her life, then it might give rise to Fourth Amendment protection of the Internet records.[132] But this showing would be particularly difficult considering the similarity to the *Smith* fact pattern; if the government can seize Smith's phone numbers without touching an "intimate area" of his personal affairs, then the FBI can likely inquire into the target's telephone and Internet activities.[133] The *Doe* court did not specify precisely what information the FBI requested, so it is difficult to assess how closely these records touched upon intimate parts of the target's life. At the very least, given the *Smith* holding, any telephone numbers the FBI requested are not protected by the Fourth Amendment under the current Supreme Court precedent as described above.

Overall, *Miller* and its progeny suggest that the target has no Fourth Amendment rights in the subpoenaed material. Based upon the assumption of risk doctrine, the records' exposure to the world defeats any abstract expectation of privacy either the target or society otherwise had in the records. But if the requested documents relay some personal information about the substance of the target's Internet activities or telephone conversations, then perhaps the situation would be distinguishable from *Miller* or *Smith*. Assuming that, on balance, the target is unlikely to receive any Fourth Amendment protection to prohibit government access to these records, the question becomes: how can Doe assert a Fourth Amendment right when the target has none?

C. *Does a National Security Letter Implicate Doe's Fourth Amendment Rights?*

As with the target, Doe's subjective and objective privacy interests must be analyzed under the same doctrinal rubric to determine if Doe has any Fourth Amendment interests in the subpoenaed materials. The *Doe* court's passing analysis did not adequately address the issue.[134]

1. Subjective Prong

Doe can demonstrate a subjective expectation of privacy relatively easily. Doe probably took steps to protect the confidentiality of the records, such as encryption or restricted access. Similarly, it is unlikely that the company ever exposed them to public view. Assuming these facts are true, Doe took sufficient action to show that the company expected the records sought by the

[131] United States v. Miller, 425 U.S. 435, 444, n.6 (1976) (quoting Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 78-79 (1974)).

[132] *Id.*

[133] *See Smith*, 442 U.S. at 744 (1979).

[134] Doe v. Ashcroft, 334 F. Supp. 2d 471, 494 n.118 (S.D.N.Y. 2004).

FBI's NSL to remain private. But, as stated earlier, the subjective prong of the *Katz* test has little dispositive value.[135]

2. Objective Prong

The more important, and more difficult analysis, is whether society is prepared to recognize Doe's privacy interest in these records. The *Katz* analysis balances Doe's sense of security against the government's need for the NSL. Like any value judgment, the road one takes depends on the outcome one wishes to achieve.[136] If the reviewing court examines the issue on appeal by measuring an NSL's impact on Doe's sense of security, the court is likely to extend the Fourth Amendment to protect these records. If, however, the reviewing court frames the issue by concerning itself with the burden on law enforcement, then it will likely find that an NSL implicates no Fourth Amendment interests.

To begin with, as the *Katz* test suggests, the question of Doe's reasonable expectation of privacy in the records should be considered apart from precedent. There are societal concerns about the government having the power to rummage through a company's records unchecked.[137] Perhaps though, because of the grave threat to national security, society is less concerned about the government's rummaging when it involves a suspected terrorist. But one might argue that society expects some modicum of governmental restraint because the target has no way of protecting the records from unwarranted government review.

Of course, Doe still has to overcome the records' public exposure in order to receive Fourth Amendment protection. Doe has not willingly exposed the records to the public, like the target has, and has even tried affirmatively to keep these documents secret. Nonetheless, the target exposed the information to Doe. The entire premise of the assumption of risk doctrine is that the government could have seen the information, just as any member of the public could.[138] But Doe has a strong counterargument that the records have only been exposed to the ISP. Therefore, law enforcement could only have access to the records with Doe's permission.

Considering that society likely expects Doe to receive some measure of protection from government intrusion into its company records, combined with the fact that Doe has not exposed the records, and the possibility of public exposure is minimal, one would think expect that Doe has a reasonable expectation of privacy in the target's records. Yet the conclusion that Doe, a

[135] *See* discussion *supra* Part II.A.2.a.

[136] LAFAVE, *supra* note 67, § 2.1(d).

[137] Again, traditionally, this unfettered government access to such information is disturbing. *See supra* note 126 and accompanying text.

[138] *See* California v. Ciraolo, 476 U.S. 207, 213 (1986) (maintaining that the law permits government "observations from a public vantage point where [an officer] has a right to be and which renders the activities clearly visible").

corporation, may exert greater rights than the target, who has personal privacy at stake, seems to defy common sense.

3. Can Doe Exert Greater Rights than the Target?

As discussed above, the target has little chance of demonstrating a legitimate expectation of privacy in the subpoenaed information.[139] This might suggest that Doe similarly has no Fourth Amendment rights; how could a corporation assert a greater privacy interest in its user's Internet activity than the user herself?[140] The Court has never directly addressed whether a corporation has any legitimate Fourth Amendment interest in its customers' Internet records.[141] Rather, as demonstrated in Part III, the Supreme Court allows a corporation to be free from "officious intermeddling" and has developed minimal requirements for any administrative subpoena.[142] These requirements are particularly relevant here, as the *Doe* court itself acknowledged that an NSL should be viewed as a type of administrative subpoena.[143]

The more general issue of a corporation's Fourth Amendment rights in its customers' records has been dealt with by the Supreme Court. In *California Bankers Ass'n v. Shultz*, the Court suggested that a corporation can acquire stronger interests than its customers, but stopped short of specifically holding so.[144] The district court in *Shultz* had concluded that sections of the Bank Secrecy Act were "repugnant to the Fourth Amendment" because it allowed

[139] *See* discussion *supra* Part II.B.

[140] There might be situations where the subscriber's activities reveal something about the ISP, but this would be a rare case and would not be applicable to *Doe*.

[141] *Cf.* Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 51 (1974) ("Whether the bank might in other circumstances rely on an injury to its depositors, or whether, instead, this case is governed by the general rule that one has standing only to vindicate his own rights need not now be decided . . . .") (citation omitted).

[142] For more detail on the relationship between the Fourth Amendment and administrative subpoenas, see *infra* Part III. At this point, it is sufficient to note that administrative subpoenas are similar to grand jury subpoenas, which Congress specifically looked to when carving out this power for the FBI. At a minimum, an administrative subpoena must pass a reasonableness test. The documents must be: (1) within the authority of the agency; (2) not too indefinite; and (3) reasonably relevant. Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946).

[143] *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004).

[144] 416 U.S. 21, 51 (1974) ("[T]he Court has allowed a party upon whom the sanction falls to rely on the wrong done to a third party in obtaining relief."). The California Bankers Association attacked the Bank Secrecy Act, 31 U.S.C. §§ 531-5332 (2000), arguing that requiring its member banks to maintain and release customer records violated their Fourth Amendment rights and the rights of their depositors. *Shultz*, 416 U.S. at 51.

the Secretary of the Treasury broad discretion in determining what information banks would be required to turn over.[145]

The Supreme Court disagreed and reversed.[146] The Court declined to decide if the depositor's rights were violated based only on a premise that a potential violation might occur in the future.[147] The Court also did not decide if the bank's interests were implicated.[148] Rather, the *Shultz* Court was satisfied that the bank's Fourth Amendment rights were not violated because the subpoena met minimal requirements and was controlled by existing legal process.[149] The requirements for administrative subpoenas suggest that a corporation has distinct interests, sufficient to give it legitimate expectation of privacy in its customers' information, even when the customer has no Fourth Amendment right.[150]

Such a conclusion contradicts the general understanding that individuals enjoy stronger Fourth Amendment rights than corporations.[151] Generally, a corporation cannot assert a right to conduct its business in secret.[152] The government allows corporations to exist; corporations have "the privilege of acting as artificial entities," in addition to being able to engage in interstate commerce.[153] Along with these "favors" from the government comes enhanced regulation, giving law enforcement a legitimate right to be satisfied that companies are behaving consistent with the law and public interest.[154] Also, the following language from *Shultz* suggests that the bank has no injury

[145] *Schultz*, 416 U.S. at 42 (stating the district court's position that "the Act could conceivably be administered in such a manner as to compel disclosure of all details of a customer's financial affairs, [and that, as a result] the domestic reporting provisions must fall as facially violative of the Fourth Amendment.").

[146] *Id.* at 77-78 (reversing "that portion of the District Court's judgment which held that the domestic reporting requirements imposed under Title II of the Act violated the Constitution").

[147] *Id.* at 51-52 ("Claims of depositors against the compulsion by lawful process of bank records involving the depositor's own transactions must wait until such process issues."). *Miller* decided this question two years later when the Court found that the depositor had no legitimate expectation of privacy. United States v. Miller, 425 U.S. 435, 444 & n.6 (1976) (discussing Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 78-79 (1974)).

[148] *See Shultz*, 416 U.S. at 69.

[149] *Id.* at 67; *see infra* Part III (discussing these minimal requirements).

[150] *See supra* note 142.

[151] *See, e.g.*, United States v. Morton Salt Co., 338 U.S. 632, 651-52 (1950) ("[T]he disparity between artificial and natural persons is so significant that differing treatment can rarely be urged as an objection to a particular construction of a statute.").

[152] *Id.*

[153] *Id.* at 652 (justifying a corporation's inability to claim an absolute right of privacy). The ultimate issue is how this reduced amount of privacy affects Doe's legitimate expectation of privacy, not the reasonableness of the process. *See infra* Part III.

[154] *See Shultz*, 416 U.S. at 66-69 (explaining that "corporations can claim no equality with individuals in the enjoyment of a right to privacy").

to protest: "Whatever wrong such a result might work on a depositor, it works no injury on the bank."[155] We know from *Miller* that there is no injury to the depositor, and so, using this logic, it seems that there is also no injury to the bank.

This incongruity between the target having no Fourth Amendment protection and Doe having some Fourth Amendment protection has yet to be resolved. Although *Shultz* suggests that banks have their own distinct Fourth Amendment interests in financial records, it also suggests that Doe's rights, as a corporation, are more limited than those of an individual's. But it is important to note that the Court decided *Shultz* before it firmly articulated the assumption of risk doctrine in *Miller*. Would the *Miller* Court have wanted to dilute its holding by allowing the bank to thwart weighty government concerns?[156] Does it make sense to allow the telephone company to keep Smith's telephone records, but not Smith himself? Or to allow the garbage company to protect Greenwood's trash, but not Greenwood?

Fixing this apparent inconsistency means either recognizing the target's Fourth Amendment rights or taking away Doe's. In order to resist handing over the documents to the government, Doe must argue that simply collecting and holding the records gave it greater and distinct expectations of privacy over the target, even after the record's exposure. This has to be done against the backdrop of both congressional intent in passing and broadening § 2709 and the overarching concern of national security.[157] The *Doe* court explicitly relied on the fact that Doe promised confidentiality to its customers, but the *Miller* analysis directly refutes such reliance.[158] In *Miller*, congressional action in enacting the Bank Secrecy Act eroded any privacy interest of the bank.[159] Similarly, here, rather than legislating against NSLs in favor of personal

---

[155] *Id.* at 51.

[156] *But see* United States v. Miller, 425 U.S. 435, 446 (1976) (implying that the banks had a separate and real Fourth Amendment interest, as the Court would consider the legitimacy of the subpoenas only if "[t]he banks [contested] their validity").

[157] *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 476 (S.D.N.Y. 2004) ("National security is a paramount value, unquestionably one of the highest purposes for which any sovereign government is ordained.").

[158] *Miller*, 425 U.S. at 442 (finding that the documents were not truly confidential because they "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business").

[159] *Id.* at 442-43:

> The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they "have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings."

(quoting 12 U.S.C. § 1829b(a)(1)(A) (2000)). *But see* California v. Greenwood, 486 U.S. 35, 44 (1988) (rejecting respondent's "suggestion that concepts of privacy under the laws of each State are to determine the reach of the Fourth Amendment").

privacy, Congress specifically defined the respective interests under § 2709,[160] and amended § 2709 knowing that the FBI would only have to meet the minimal requirements for administrative subpoenas.[161]

Even though it might strain common sense to understand how Doe can have a greater interest in the target's information than the target himself, this seems to be the state of the law. Although the target has no Fourth Amendment protection for records that detail his Internet use, the Supreme Court affords Doe protection against unreasonable subpoenas. The remainder of this Note assumes that only Doe has a Fourth Amendment interest in the records, and that the NSL is a "search or seizure" with respect to Doe. The government's actions must now be considered under the well-developed administrative subpoenas doctrine to answer the question: was the NSL reasonable?

III. WAS THE *DOE* NATIONAL SECURITY LETTER A REASONABLE SEARCH OR SEIZURE?

After satisfying the threshold issue of who has an interest in the records protected by the Fourth Amendment, the next question is: what level of Fourth Amendment protection should Doe receive? As discussed, the *Doe* court and Congress have treated NSLs as tantamount to administrative subpoenas.[162] This comparison is not exact; the *Doe* court noted that NSLs "constitute a unique form of administrative subpoena cloaked in secrecy and pertaining to national security interests."[163] But these differences aside, as long as courts and Congress view NSLs as a species of administrative subpoena, then determining the NSL's reasonability incorporates administrative law.

Two issues predominate here. First, did the NSL comport with the minimal administrative subpoena requirements? And second, was the process fair to Doe, sufficiently allowing for judicial review? If the answer to both questions

---

[160] This action by Congress is relevant to Doe's interests in the information as well, as this legislation also could reduce the significance of any reliance Doe placed on the confidentiality of the records.

[161] *See* 18 U.S.C. § 2709 (2000 & Supp. 2002), *invalidated by* Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004). Congress is well aware of agency power to issue subpoenas as evidenced by the numerous statutes that authorize such activity. *See* Charles Doyle, *Administrative Subpoena and National Security Letters in Criminal and Foreign Intelligence Investigations*, RL32880, CONG. RES. SERV. CRS-1 (Apr. 15, 2005), *available at* http://www.fas.org/sgp/crs/natsec/RL32880.pdf (reviewing Congressional uses, amendments, and discussions of administrative subpoenas and national security letters).

[162] *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004); S. REP. NO. 104-258, at 21 (1996), *as reprinted in* 1996 U.S.C.C.A.N. 3945, 3966 (describing the national security letter under § 2709 as an administrative subpoena); H.R. CONF. REP. NO. 104-832, at 38 (1996), *as reprinted in* 1996 U.S.C.C.A.N. 3996, 4003; STAFF OF S. COMM. ON INTELLIGENCE, 109TH CONG., REPORT ON THE USA PATRIOT ACT OF 2001 (discussing national security letters as administrative subpoenas), *available at* http://intelligence.senate.gov/report_usapatriot_act.htm.

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

is yes, then the NSL was a reasonable search and seizure and § 2709, at least as applied to Doe, is constitutional.

A. *Reasonableness Standard for Administrative Subpoenas*

Administrative subpoenas are not subjected to the same rigor as search warrants.[164] Rather than the target receiving the search warrant as the government seizes evidence, Doe receives a subpoena that demands the corporation hand over the evidence. Although both processes implicate Fourth Amendment interests, a corporation subjected to a subpoena receives much less protection than an individual subjected to a search warrant.[165] The Supreme Court has recognized that a corporation should not be afforded as much Constitutional protection as an individual, while simultaneously recognizing the congressional intent to grant administrative agencies comprehensive investigatory powers.[166] These investigatory powers have become more vital as companies, commerce, and statutes have become increasingly sophisticated.[167] Therefore, to allow agencies to effectively regulate in their field according to the wishes of Congress, the Supreme Court is very tolerant of administrative subpoenas.[168]

This tolerance did not always exist. Over a century ago, *Boyd v. United States* limited the government's access to subpoenaed documents.[169] The Court found an unreasonable search or seizure when the government compelled the production of private papers that would effectively force Boyd

---

[164] *See Miller*, 425 U.S. at 445-46 & n.8.

[165] *See* United States v. Morton Salt Co., 338 U.S. 632, 651-52 (1950); *see also supra* Part II.C.3.

[166] LAFAVE, *supra* note 67, § 14.3.

[167] *See, e.g.*, Branzburg v. Hayes, 408 U.S. 665, 688 (1972) (explaining that because a grand jury must return well-supported indictments, "its investigative powers are necessarily broad").

[168] *See Morton Salt Co.*, 338 U.S. at 640-42 (1950) (rationalizing that "[Administrative] agencies are expected to ascertain when and against whom proceedings should be set in motion and to take the lead in following through to effective results"). The concern voiced most often against administrative subpoenas is that the Fifth Amendment privilege against self-incrimination might be violated through the production of materials. But this privilege does not apply to corporations. *See* Fisher v. United States, 425 U.S. 391, 424-25 (1976); United States v. White, 322 U.S. 694, 700 (1944); Hale v. Heinkel, 201 U.S. 43, 75 (1906), *overruled in part by* Murphy v. Waterfront Comm'n, 378 U.S. 52 (1964). Some argue that when there is no Fifth Amendment protection, more protection should be available under the Fourth Amendment, or alternatively, the Due Process Clause. *See In re* Grand Jury Proceedings, 601 F.2d 162, 170 n.5 (5th Cir. 1979); *In re* Horowitz, 482 F.2d 72, 75-79 (2d Cir. 1973).

[169] Boyd v. United States, 116 U.S. 616, 621-22 (1886) (holding that being an object of a subpoena is tantamount to a search or seizure and that the Fourth Amendment therefore applies), *abrogated by* Fisher v. United States, 425 U.S. 391 (1976).

to be a witness against himself.[170] But any continuing reliance on *Boyd* is ill-advised. As one blunt commentator said, "*Boyd* is dead."[171] The Supreme Court has narrowed the opinion ever since it was handed down.[172] *Boyd*'s holding, relating to subpoenas, has now been replaced by a body of law, as described below, that sets a very low threshold of reasonableness.

Under the current standard, an administrative subpoena violates the Fourth Amendment only if the subpoena does not comply with certain minimum requirements. The Supreme Court first outlined these requirements in *Oklahoma Press Publishing Co. v. Walling*.[173] In that case, the Court relied heavily on two considerations to determine how rigorous subpoena requirements should be. First, Congress had specifically granted agencies this broad subpoena power.[174] Second, a corporation enjoys fewer rights than a private individual.[175] Thus, any overly stringent standards would frustrate congressional goals in allowing administrative agencies to effectively regulate. The Fourth Amendment clearly trumps any impermissible congressional decree, but Congress can exercise wider investigative powers over corporate entities.[176] Therefore, Congress can authorize agencies to investigate a broad range of activities, even with only a minimal level of suspicion.

The agency, however, cannot investigate just anything; the Court crafted minimum requirements designed to curb potential abuses and protect against unreasonable agency demands. An administrative subpoena is proper and enforceable if it describes with "particularity," and in sufficiently definite

---

[170] *Id.* at 634-35:

> We are further of the opinion that a compulsory production of the private books and papers . . . is compelling him to be a witness against himself, within the meaning of the fifth amendment to the constitution, and is the equivalent of a search and seizure – and an unreasonable search and seizure – within the meaning of the fourth amendment.

[171] Stan Krauss, Note, *The Life and Times of* Boyd v. United States *(1886-1976)*, 76 MICH. L. REV. 184, 212 (1977).

[172] Although the holding has never been formally overturned, the Supreme Court itself has questioned how much of *Boyd* remains good law. *Fisher*, 425 U.S. at 407 ("Several of Boyd's express or implicit declarations have not stood the test of time."). In *Fisher*, the Court noted specifically that "[t]he application of the Fourth Amendment to subpoenas" has been limited by several subsequent decisions. *Id.* (citations omitted).

[173] Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 208-09 (1946).

[174] *Id.* at 197-98 ("[T]he statute's language leaves no room to doubt that Congress intended to authorize just what the Administrator did and sought to have the courts do.").

[175] *Id.* at 204-05. Again, as an example, a corporation cannot claim a privilege against self-incrimination. Hale v. Heinkel, 201 U.S. 43, 75 (1906), *overruled in part by* Murphy v. Waterfront Comm'n, 378 U.S. 52 (1964); *see also supra* Part II.C.3. (discussing California Bankers Ass'n v. Shultz, 416 U.S. 21 (1974)).

[176] *See* United States v. Morton Salt Co., 338 U.S. 632, 652 (1950) (justifying a corporation's inability to claim an absolute right of privacy); *see also supra* Part III.C.3 (discussing reasons why a corporation receives less Fourth Amendment protection than an individual).

terms, the items to be produced;[177] if the agency issuing the subpoena is authorized by law to demand the information; and if the materials specified are relevant to the investigation.[178] The Court believed these minimum requirements struck the proper balance between a corporation's interest in freedom from "officious intermeddling" and Congress' interest in ensuring that the law is being followed.[179]

These lenient requirements have been affirmed and reinforced by later decisions. In *United States v. Morton Salt Co.*, the Court acknowledged that an administrative agency has a right to know whether "corporate behavior is consistent with the law and the public interest."[180] The Court extrapolated the requirements from *Walling* and held that an administrative subpoena comports with the Fourth Amendment if: (1) the investigation "is within the authority of the agency"; (2) the subpoena "is not too indefinite"; and (3) the subpoena is seeking relevant information.[181] The agency should use the information gathered under the order to determine if there is a violation of the law.[182] The Court was clear to note that "the only power [the agency has] is the power to get information from those who best can give it and who are most interested in not doing so."[183]

B. *Application of Administrative Subpoena Requirements to a National Security Letter*

Because it categorized an NSL as an administrative subpoena for its analysis, the *Doe* court was remiss in not thoroughly evaluating the NSL under

[177] *Walling*, 327 U.S. at 209.

[178] The Court went on to say that "[i]t is enough that the investigation be for a "lawfully authorized purpose, within power of Congress to command." *Id.* In *Walling*, the Court equated the subpoena to a warrant by suggesting that there were probable cause and particularity requirements. *Id.* Probable cause is found when "the "investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry." *Id.* Particularity is found when the "specification of the documents to be produced [is] adequate, but not excessive, for the purposes of the relevant inquiry." *Id.*

[179] *Id.* at 213-14 (finding that the balance between these interests must tip in the government's favor because "Congress has authorized the Administrator, rather than the district courts in the first instance, to determine the question of coverage in the preliminary investigation of possibly existing violations").

[180] *Morton*, 338 U.S. at 652 (1950). In *Morton*, the Federal Trade Commission (FTC) had obtained a judgment against Morton Salt and other defendants in an earlier suit demanding compliance with certain trade practices. *Id.* at 635-36. To determine if Morton Salt was complying with the judgment, the FTC subpoenaed records in connection with the pricing, producing, and marketing of salt. *Id.*

[181] *Id.* at 652-53. Before a court will deem an order arbitrarily excessive, the supplicant must "have made reasonable efforts before the [C]ommission itself to obtain reasonable conditions." *Id.* at 653-54.

[182] *See id.* at 652.

[183] *Id.*

this rubric.[184] Before considering the specific requirements applicable to an NSL, it is worth noting that the policies underlying the breadth of *Walling*'s minimum requirements are present in relation to NSLs as well.[185] Congress specifically granted the FBI the power to issue NSLs in § 2709, and Doe, as a corporation, enjoys less Fourth Amendment protection than an individual.[186] This suggests the NSL is reasonable as well, and is bolstered by the fact that the NSL, as demonstrated below, easily complies with *Walling*'s specific administrative subpoena requirements. Even though the Supreme Court has expressly said that any inquiry into the reasonableness of a subpoena cannot be broken down into a precise mathematical formula, the three *Walling* requirements continue to form the bedrock of the judicial analysis.[187]

1. Authorized Purpose of the Investigation

The authorized purpose prong raises only a nominal concern for the government. Generally, an administrative agency has broad investigatory powers.[188] And courts often liberally read statutes in authorizing administrative investigations, allowing for broad inquiries.[189] The party attacking the subpoena bears a heavy burden to persuade a court that the agency's investigation has no authority.[190]

---

[184] Doe v. Ashcroft, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004). While the Court noted the general requirements for administrative subpoenas, it did not apply them to the particulars of the case. *See id.* at 495.

[185] *See supra* text accompanying notes 173-174.

[186] *See supra* Part I.A (discussing the legislative history and powers granted under § 2709); text accompanying notes 151-154 (explaining that the Fourth Amendment affords individuals stronger protection than corporations).

[187] *See* McConnell v. FEC, 540 U.S. 93, 237 (2003) (citing *Walling* in support of "broad governmental authority for agency information demands from regulated entities"); Packwood v. Senate Select Comm. on Ethics, 510 U.S. 1319, 1319 (1994) (citing *Walling* for the proposition that reasonableness "cannot be reduced to [a] formula," and thereby recognizing the continuing validity of *Walling*). *Miller* recognized the *Walling* standards, but did not apply them because the bank did not contest the validity of the subpoenas. *See* United States v. Miller, 425 U.S. 435, 445-46 & n.9 (1976).

[188] LAFAVE, *supra* note 67, § 4.13(b), at 728-29 ("The Supreme Court has sanctioned the broad investigatory powers of administrative agencies . . . .").

[189] *Id.* ("[T]he trend in recent years has been for the courts to adopt liberal interpretations of statutory provisions authorizing investigation."); *see also Morton Salt*, 338 U.S. at 642-43 (analogizing an agency's power to conduct investigations to a Grand Jury, which "can investigate merely on suspicion that the law is being violated, or even just because it wants assurance that it is not").

[190] *See In re* Grand Jury Subpoenas Duces Tecum Addressed to Certain Executive Officers of the M.G. Allen & Assoc., 391 F. Supp. 991, 995 (D.R.I. 1975) ("If the Government can establish to the Court's satisfaction that the documents requested have some general relevance to a legitimate grand jury investigation, said prima facie showing of relevance becomes irrebuttable."); LAFAVE, *supra* note 67, § 4.13(b), at 727.

In *Doe*, the FBI certified in its NSL that the information sought was relevant to an authorized terrorist investigation.[191] Under § 2709, this was sufficient to show that the FBI investigation was authorized.[192] Although simply relying on the FBI's certification is slightly disconcerting, it would be improper for the court to address that concern here. The narrow question is whether Congress authorized this type of investigation, not whether the authorization was adequate.[193]

Because Congress specifically authorized the use of NSLs through the framework in § 2709, and the FBI is lawfully authorized to hunt down clandestine terrorist activities, there can be little question that the purpose behind the Doe investigation was authorized.[194] Therefore, the *Doe* NSL meets the first *Walling* requirement.

2. Relevance of Documents to the Inquiry

The FBI is not authorized to subpoena any document it desires. Rather, the document must be relevant to the FBI's general inquiry.[195] The *Doe* court does not detail the specifics of the NSL or explain which specific documents the FBI sought, nor does the government defend why the requested documents are relevant to the inquiry.[196] But, like authorized purpose, this requirement has been broadly construed, and the government should not face a significant challenge.[197] Any motion to quash a subpoena must be denied unless the court concludes "that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject

[191] *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 478-79 (S.D.N.Y. 2004).

[192] *See* 18 U.S.C. § 2709 (2000 & Supp. 2002), *invalidated by* Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004); *Doe*, 334 F. Supp. 2d at 480-84.

[193] *See supra* Part III.A.1. This general question would normally be subsumed within the reasonableness analysis, but the Supreme Court already implicitly incorporated such balancing when it outlined the *Walling* requirements.

[194] *See Morton Salt*, 338 U.S. at 642-43 ("When investigative and accusatory duties are delegated by statute to an administrative body, it . . . may take steps to inform itself as to whether there is probable violation of the law.").

[195] *See* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946); LAFAVE, *supra* note 67, § 4.13(c), at 729.

[196] *See Doe*, 334 F. Supp. 2d at 478-79.

[197] *See In re* Grand Jury Investigation, 381 F. Supp. 1295, 1298 (E.D. Pa. 1974) (holding that "only in an extreme case of a clear showing of unreasonableness, of abuse of power by the Government, will a court be induced to quash . . . [a] subpoena on the ground that it is overly burdensome"). In many cases, the application of a relevance test is subjective and based largely on a relationship between the general information being sought and the particulars of the documents.

of the . . . investigation."[198] Indeed, Doe never questioned this requirement, apparently assuming the documents were relevant.[199]

The FBI's general inquiry in *Doe* is whether the target is a terrorist, and if so, in what activities he is engaged.[200] A reasonable probability exists that examining an individual's Internet activity will produce information relevant to this inquiry. Therefore, the FBI requested relevant documents, and the NSL meets the second *Walling* requirement.

3. Adequate Specification

The NSL must specify the documents Doe is to produce.[201] The adequate specification requirement has two prongs.[202] First, although the level of specificity does not have to be "excessive,"[203] the subpoena must provide a "sufficiently definite description of the documents" to reasonably inform the recipient which documents must be produced.[204] Second, the subpoena cannot "be so broad that compliance with its terms is unduly burdensome."[205] As with all other *Walling* requirements, the burden is on the party attacking the subpoena to show that the provided specification in the subpoena is not adequate.[206]

Because agencies do not always know precisely what they hope to find through a subpoena, courts are reluctant to demand too much specificity or force the agency to detail more than it knows.[207] Courts look to the facts and circumstances of each case to determine the adequacy of the specification.[208] The first part of this test, whether the subpoena is sufficiently definite, rarely presents an issue.[209] Occasionally, courts will quash subpoenas that have broad language such as "all conceivably relevant papers."[210] But the subpoena

[198] United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991) (establishing that the court must deem a subpoena relevant unless no reasonable possibility exists that the documents sought are relevant to the investigation).

[199] *See supra* text accompanying note 184.

[200] *Doe*, 334 F. Supp. 2d at 478-79.

[201] *See* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946).

[202] LAFAVE, *supra* note 67, § 4.13(d), at 737.

[203] *Walling*, 327 U.S. 186, 209 (1946) (suggesting that the "purposes of the relevant inquiry" must be considered when deciding what is excessive).

[204] LAFAVE, *supra* note 67, § 4.13(d), at 737.

[205] *Id.*

[206] *Id.*

[207] *Id.*

[208] *See In re* Eastman Kodak Co., 7 F.R.D. 760, 763 (1947) ("What is reasonable is determined by no fixed standard, but by the circumstances shown in respect to each case.").

[209] LAFAVE, *supra* note 67, § 4.13(d), at 737.

[210] *Id.* at 738; *see* United States v. Dauphin Deposit Trust Co., 385 F.2d 129, 131 (3d Cir. 1967) (quashing part of a summons from the IRS that sought records of "transactions of any

can be saved by simply adding a limitation that requires production of documents "known to the subpoenaed party."[211]

In *Doe*, the NSL sought only records concerning the target of the investigation.[212] The FBI did not seek information either about the company or about a significant number of subscribers. Given the focus of this investigation, Doe is unlikely to meet his heavy burden of showing that the description was not sufficiently definite.

The second, and most frequently litigated, component regarding the adequacy of specification in subpoenas and NSLs is whether the requested production is too cumbersome for the subpoenaed party.[213] Generally, parties attack the quantity of documents demanded or the length of the time period the government seeks to review.[214] Courts have developed three factors to determine if a subpoena is unduly burdensome. First, the breadth of the subpoena must be related to the scope of the investigation.[215] The broader the underlying investigation, the more leeway the government will have in compelling production.[216] Second, courts examine the likelihood that the documents requested will produce evidence helpful to the investigation, often by asking if the documents are reasonably relevant to the investigation.[217] Lastly, and most importantly, courts consider the financial burden imposed on the corporation as a result of compliance.[218] This is heavily fact-specific to the case in question given that a large enterprise can produce many documents without suffering much financial burden, a similar request of a smaller enterprise would be financially harder.[219]

Using these three factors, the NSL qualifies without much difficulty as not being too burdensome. First, the FBI seeks information only about the specific

nature [between 1961 and 1964] handled by the bank on behalf of [its customers]") (citation and quotation marks omitted).

[211] LAFAVE, *supra* note 67, § 4.13(d), at 738; *see In re* Radio Corp. of Am., 13 F.R.D. 167, 171 (S.D.N.Y. 1952) (suggesting that limiting the language and scope of a subpoena "particularly weaken[s] the force of [any] objection").

[212] *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 478-79 (S.D.N.Y. 2004).

[213] LAFAVE, *supra* note 67, § 4.13(d), at 739.

[214] *Id.*

[215] *Id.* at 740 (explaining that "the scope of the investigation helps determine the volume of documents that must be produced").

[216] *Id.*; *see also* People v. Allen, 103 N.E.2d 92, 95-96 (Ill. 1951) (reviewing numerous Supreme Court decisions and finding that they stand for the proposition that "the permissible breadth of a *subpoena duces tecum* is to be measured by the scope of the problem under investigation").

[217] LAFAVE, *supra* note 67, § 4.13(d), at 740 (describing the overlap between this factor and the relevance prong and explaining that "[i]f the papers demanded are clearly relevant to the investigation, the courts are more inclined to enforce broad subpoenas").

[218] *Id.*

[219] *In re* Radio Corp. of Am., 13 F.R.D. 167, 172 (S.D.N.Y. 1952) (stating that "[i]nconvenience is relative to size").

target, sufficiently tailoring the scope of their investigation. Second, as mentioned earlier, it is reasonably likely that, if the target is in fact in terrorist operations, some evidence of that would appear in his Internet activity held by Doe.[220] Lastly, Doe's NSL sought "certain information" related to the target's Internet activity.[221] It is likely that all information pertinent to one subscriber is kept in one or two easily accessible locations within the company's records. Both a telecommunications company and an ISP are likely to have an electronic recording of the type of information the government sought, rather than a large unorganized filing cabinet of everyone's Internet activity. Therefore, it is unlikely that the request will pose an unreasonable financial burden on Doe, and certainly it will not threaten the vitality of the corporation. Thus, the *Doe* NSL satisfies both parts of the adequate specification requirement because it provides a definite description of the records requested and is not unduly burdensome, and the NSL meets the third and final *Walling* requirement.

As an administrative subpoena, the NSL in *Doe* satisfies the minimal *Walling* requirements. First, the FBI issued the NSL for an authorized purpose. The NSL specified that the FBI needed certain information for an investigation to protect against terrorist activities, and Congress specifically authorized this stated purpose when it passed § 2709.[222] Second, the documents the FBI sought were relevant to this investigation because the target's Internet activity is likely to help uncover anything nefarious that the target was plotting and confirm or disprove the FBI's suspicions. Finally, the NSL was sufficiently specific because it narrowed the documents requested to a specific investigation and is likely not to financially burden the company.[223] Accordingly, even if the NSL implicates Doe's Fourth Amendment interests, it does so reasonably.

C. *Did the National Security Letter in* Doe *Provide for Adequate Judicial Review?*

Even if an administrative subpoena satisfies the *Walling* requirements, it cannot intrude upon or usurp the court's adjudicatory powers.[224] A court must have the opportunity to review the facts and circumstances of each subpoena to

[220] *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 478-79 (S.D.N.Y. 2004).

[221] *Id.* at 478.

[222] *Id.*; *see* 18 U.S.C. § 2709 (2000 & Supp. 2002), *invalidated by* Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

[223] *See Doe*, 334 F. Supp. 2d at 478-79.

[224] *Id.* at 495 ("[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* See v. City of Seattle, 387 U.S. 541, 545 (1967) ("[T]he subpoenaed party may obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply.").

ensure that it is reasonable.[225] Therefore, if § 2709 precludes judicial review then it violates the Fourth Amendment and any NSL issued under the section would be unconstitutional.

This preclusion can manifest itself in two ways: (1) § 2709 itself might forbid review, or (2) the tone of the NSL might be so coercive as to practically stop any NSL recipient from enlisting the help of the judiciary.[226] The *Doe* court was especially concerned with the availability of judicial review under § 2709,[227] because it believed that most NSL recipients would not object to an otherwise unreasonable NSL and seek judicial review.[228] Thus, the lack of judicial review was precisely why the *Doe* court held that § 2709 was unconstitutional.[229] The *Doe* court's analysis failed to note that judicial review has been implied where statutes have not explicitly provided for it; this, coupled with the lack of substantial review of the *Walling* factors, casts doubts on the court's conclusions.

1. Does § 2709 Forbid Judicial Review?

One of the *Doe* court's primary concerns with the constitutionality of § 2709 was that the section did not explicitly provide for judicial review. The *Doe* court's analysis relied on a comparison of § 2709 to other statutes that authorize administrative subpoenas and NSLs.[230] Yet none of the other statutes authorizing NSLs cited by the *Doe* court explicitly provide the subpoenaed party the opportunity to seek judicial review.[231] In fact, courts have upheld statutes that are similarly silent on judicial review.[232] Several of the statutes, however, do state that the government may seek judicial enforcement of the subpoena,[233] and one provides a penalty beyond contempt for parties that do not comply.[234] It would be a strange result indeed if the government could force a subpoenaed party in front of a district court for

[225] Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 217 (1946) (explaining that administrative subpoenas must be subject to "judicial supervision" and "surrounded by every safeguard of judicial restraint").

[226] *See Doe*, 334 F. Supp. 2d at 495-96.

[227] *Id.* at 492.

[228] *Id.* at 502 ("For the reasonable NSL recipient confronted with the NSL's mandatory language and the FBI's conduct related to the NSL, resistance is not a viable option.").

[229] *Id.* at 506.

[230] *Doe*, 334 F. Supp. 2d at 492-94.

[231] *Id.*; *see also supra* note 31.

[232] *See* United States v. Morton Salt Co., 338 U.S. 632, 635 (1950).

[233] 7 U.S.C. § 4610a(c) (2000) (providing for judicial enforcement of subpoenas issued by the Secretary of Agriculture); 12 U.S.C. § 3416 (2000 & Supp. 2002) (providing for court review of subpoenas issued to banks and financial institutions); 15 U.S.C. § 78u(c) (2000) (providing for judicial enforcement of SEC-issued subpoenas).

[234] 15 U.S.C. § 1681u (2000 & Supp. 2002) ("[I]njunctive relief shall be available to require compliance with the procedures of this section.").

enforcement purposes, but the subpoenaed party was forced to stand mute, unable to contest the reasonability of a subpoena.[235] Therefore, the cited statutes likely imply that both the government and the subpoenaed party can seek judicial redress.[236]

Moreover, even though § 2709 did not explicitly provide for judicial review, the Supreme Court has suggested that a court always has jurisdiction to review an administrative subpoena.[237] Like § 2709, the statute at issue in *Morton Salt* did not explicitly provide for any judicial review or control.[238] In that case, the recipient was fearful that an administrative subpoena might fall below the minimum requirements of *Walling* and yet be practically unrestrained if a recipient could not seek judicial review.[239] The *Morton Salt* Court was not persuaded, intimating that the absence of judicial review in the statute does not necessarily preclude a court's ability to review judicial orders, but reserving that specific question for another day.[240]

Morton Salt was not the only time the Supreme Court addressed a court's supervisory powers over subpoenas. In *United States v. Powell*, the Supreme Court found that judicial review was presumed in the particular administrative subpoena statute before it.[241] While the IRS could seek judicial enforcement of its administrative subpoena, the subpoenaed party "may challenge the summons on any appropriate ground."[242] In *See v. City of Seattle*, the Court, in discussing the caselaw applicable to administrative subpoenas, noted that judicial review is generally available to determine an administrative subpoena's reasonableness.[243] The subpoenaed party may always seek judicial

[235] *See infra* notes 243-244 and accompanying text.

[236] *See also Morton Salt*, 338 U.S. at 654 (expressing, in dictum, that administrative subpoena statutes that do not provide for judicial review do not deny district courts an opportunity to evaluate).

[237] *See id.* at 640 (1950) ("To protect against mistaken or arbitrary [administrative] orders, judicial review is provided."); *see also* See v. City of Seattle, 387 U.S. 541, 545 (1967) ("[T]he subpoenaed party may obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply.").

[238] *Morton Salt*, 338 U.S. at 635 n.1 (detailing the statute in question, which provides for judicial enforcement but not review).

[239] *Id.* at 654.

[240] *Id.* (commenting simply that the Court was not prepared to say that it "would be powerless" if the government delayed judicial review by refusing to bring action to enforce the subpoena).

[241] United States v. Powell, 379 U.S. 48, 58 (1964). ("It is the court's process which is invoked to enforce the administrative summons and a court may not permit its process to be abused.") (citation omitted). The Court also found that the party attacking the subpoena had the burden to show an abuse of process. *Id.*

[242] *Id.* (quoting Reisman v. Caplin, 375 U.S. 440, 449 (1964)).

[243] 387 U.S. at 545 ("[T]he subpoenaed party may obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply.").

review if there is any doubt.[244] Lower courts should, however, exercise judicial restraint and be wary about overturning such subpoenas.[245]

Although nothing in § 2709 explicitly provides for judicial review, nothing explicitly forbids it either.[246] Other administrative subpoena and NSL statutes are similarly silent on the subject. When faced with such ambiguity, the Supreme Court has intimated that a district court can review an administrative subpoena. Therefore, even though § 2709 does not specifically grant Doe his day in court, he obtains review by implication. Just as the S.D.N.Y. was free to review Doe's case, a district court has the power to review any NSL to ensure it is a reasonable search or seizure.

2. Was Doe Coerced?

Even if judicial review is presumed, however, the FBI still cannot coerce compliance and practically preclude the subpoenaed corporation from seeking a court's help. The NSL Doe received did not explicitly notify him that a court has the inherent power to review the reasonability of any NSL or administrative subpoena.[247] Rather Doe was prohibited:

> "from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions." Doe was "requested to provide records responsive to [the] request personally" to a designated individual, and to not transmit the records by mail or even mention the NSL in any telephone conversation.[248]

The district court found that this harsh language, with no notice of judicial review, was tantamount to compulsion; most NSL recipients, unaware of their right to seek redress through the courts, would simply comply given the NSL's demanding language.[249]

Ironically, the fact that Doe sought and obtained judicial review suggests that the opportunity for judicial review under § 2709 is sufficiently implied to

---

[244] *Id.* at 544-45:

> In addition, while the demand to inspect may be issued by the agency, in the form of an administrative subpoena, it may not be made and enforced by the inspector in the field, and the subpoenaed party may obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply.

[245] Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 217 (1946) (stating that any arguments challenging the reasonableness of a subpoena must be "surrounded by every safeguard of judicial restraint").

[246] 18 U.S.C. § 2709 (2000 & Supp. 2002), *invalidated by* Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

[247] *Doe*, 334 F. Supp. 2d at 494 (describing the failure of both the NSL and the FBI to inform Doe that judicial review was available).

[248] *Id.* (citations and emphasis omitted).

[249] *Id.* at 494, 501-02 (holding § 2709 unconstitutional because it coerces recipients into immediate compliance without ensuring adequate process for judicial review).

put a reasonable person on notice.[250] While the district court thought that Doe was an exception to the rule, and that most people would not have sought legal advice,[251] its reasoning on this point is weakened by the assumption that lawyers would quickly be consulted. Telecommunications companies are sophisticated parties and subject to extensive regulation, often employing in-house counsel. The vast majority of their interactions with regulatory bodies occurs through lawyers. When the NSL recipient seeks legal advice, then a competent attorney should know to attack any unreasonable subpoena.[252]

Courts, including the Southern District of New York, have dealt with judicial review, subpoenas, and compulsion before. In *In re Nwamu*, FBI agents served a subpoena for "immediate production," enforced the subpoena with threats of contempt, and physically seized the documents and materials in the face of a refusal to comply.[253] The court found that the subpoenaed party's opportunity to quash the subpoena was "circumvented, frustrated and effectively foreclosed."[254]

The Second Circuit distinguished *Nwamu* in *United States v. Lartey*, where the defendant argued that he was denied an opportunity to quash because the subpoenas were served in a "coercive fashion" immediately after his arrest.[255] The *Lartey* Court disagreed and found that the government agents used no threats of contempt or physical force.[256] It did not believe the government's conduct was like that in *Nwamu*, where agents treated the subpoena as if it were a search warrant.[257]

---

[250] *See id*. at 479.

[251] *Id.* at 503.

[252] Even if an attorney was unaware of the *Walling* or *Morton Salt* opinions, the Federal Rules of Criminal Procedure clearly allow for a party to seek judicial review. FED. R. CRIM. P. 17(c)(2) (stating in part "[o]n motion made promptly, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive"). Most Fourth Amendment challenges regarding subpoenas will fail. That an attorney might be reluctant to waste resources trying to quash a subpoena implicates the low standards of administrative subpoenas, not § 2709.

[253] 421 F. Supp. 1361, 1365 (S.D.N.Y. 1976).

[254] *Id.* at 1365-67 (holding "that compliance with the subpoenas would be unreasonable and oppressive . . . and that the agents' taking of the subpoenaed items constitute[d] an unreasonable and unlawful search and seizure"). However, the Sixth Circuit has questioned the reasoning of *Nwamu*. *See* United States v. Susskind, 965 F.2d 80, 87 (6th Cir. 1992).

[255] United States v. Lartey, 716 F.2d 955, 960, 962 (2d Cir. 1983).

[256] *Id.* at 962.

[257] *Id.* (asserting that the agents in *Nwamu* treated the subpoena like a search warrant because they seized the requested items and threatened contempt); *see also* United States v. Biswa Overseas Co., 1979 U.S. Dist. LEXIS 11973, at *8 (S.D.N.Y. June 4, 1979) (deciding that government agents' conduct rose to the level of an unlawful search and seizure where they used coercion and deceit as they demanded the immediate production of documents under threat of legal sanctions, where none were authorized).

Some of the factors courts look for are any actual "coercion, compulsion, or aggressive tactics."[258] In *United States v. Triumph Capital Group, Inc.*, the court did not find any of these and held that defendants were not "deprived of any meaningful opportunity . . . to challenge the validity of the . . . subpoena,"[259] because the defendants had "sufficient time and opportunity to file a motion and, in fact, did file one."[260] In *United States v. Barr*, the court explained that "the focus of the inquiry relates to the level of compulsion present when the subpoena duces tecum is served."[261] Some relevant factors in determining the level of compulsion include: (1) the circumstances under which the subpoena is served; (2) whether agents use "force or threats of violence"; and (3) whether the subpoenaed party is given notice.[262] Lack of notice alone might not rise to a level of compulsion sufficient to find that the government action improperly impinged one's Fourth Amendment rights.[263]

The Eighth Circuit has upheld a subpoena where the defendant had not consulted with an attorney before complying.[264] Nevertheless, because the Court found that he had "ample opportunity to do so," it held that the subpoenaed party had complied voluntarily with the request.[265] In addition, the court found no evidence of coercion or seizure and thus distinguished *Nwamu*.[266]

Reviewing the above standards, the FBI acted properly.[267] It is a difficult analogy to say that the demanding language of the NSL was tantamount to the compulsion in *Nwamu*. There was no actual coercion, no compulsion, and no aggressive tactics. In *Nwamu*, the FBI agents threatened contempt, which was outside their authority.[268] In *Doe*, the FBI warned that noncompliance was prohibited by law, but unlike *Nwamu*, this was authorized and supported by statute.[269] In *Nwamu*, the court found the government agents' *actions* rose to

[258] *See* United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 55 (D. Conn. 2002).

[259] *Id.*

[260] *Id.*

[261] United States v. Barr, 605 F. Supp. 114, 117 (S.D.N.Y. 1985).

[262] *Id.*

[263] *Id.* at 118.

[264] United States v. Allison, 619 F. 2d 1254, 1264-65 (8th Cir. 1980) (upholding a subpoena despite its recipient's failure to contact an attorney).

[265] *Id.* at 1264-65 (finding "a vast difference between a misrepresentation of legal authority and a misunderstanding of legal authority").

[266] *Id.* at 1265.

[267] *See infra* notes 253-266 and accompanying text (discussing standards used by courts to determine whether a subpoena is coercive); *see also* United States v. Lartey, 716 F.2d. 955, 962 (2d Cir. 1983).

[268] *In re* Nwamu, 421 F. Supp. 1361, 1365 (S.D.N.Y. 1976) (explaining that the agents had the authority only to serve, not enforce, the subpoena).

[269] Doe v. Ashcroft, 334 F. Supp. 2d 471, 478-79 (S.D.N.Y. 2004).

the level of an illegal seizure.[270] In *Doe*, the government threatened, but took no action while it waited for Doe to comply (which he never actually did).[271] The FBI agents did not seize the requested documents and they gave Doe notice.[272] In addition, Doe not only had time to consult an attorney, but he actually did so.[273] It is permissible to contact counsel, even when a statute otherwise requires secrecy.[274] Even if Doe had not retained counsel, other circuits have held there is no coercion if the subpoenaed party had ample time to contact an attorney but failed to do so.[275] The government did demand that Doe comply with the NSL,[276] but this will happen in every situation. Congress did not intend the FBI to be in the business of politely requesting the subpoenaed party to produce documents at its leisure. While the *Doe* court was quite concerned about the harsh language of the NSL,[277] it is also difficult to see how mere language rises to a level of compulsion similar to an unreasonable search and seizure, especially considering that recipients are often sophisticated companies with access to legal advice.

In answering the question of whether the *Doe* NSL is a reasonable search and seizure under the Fourth Amendment, the NSL must be found to meet the minimum requirements for an administrative subpoena in *Walling*; to allow for judicial review; and not to be coercive in its compliance requirements. The NSL satisfies these requirements. Judicial review is implied in § 2709.[278] And there was no actual coercion by the FBI, nor was the language of the NSL coercive as courts have defined that term in the administrative subpoena context. The Fourth Amendment allows the FBI the power to compel telecommunications companies to produce subscriber records upon mere self-certification that the subscriber is a suspected terrorist. Thus, the NSL is a reasonable search or seizure.

CONCLUSION

In late 2004, the Southern District of New York invalidated 18 U.S.C. § 2709 after it found that the statute violated the Fourth Amendment.[279] The essential issue on appeal is whether § 2709 authorizes an unreasonable search and seizure. The first inquiry in any Fourth Amendment analysis is whether the party reasonably expected the information to remain private. In *Doe*, the

[270] *See Nwamu*, 421 F. Supp. at 1367 ("[T]he agents' taking of the subpoenaed items constitute[d] an unreasonable and unlawful search and seizure.").

[271] *Doe*, 334 F. Supp. 2d at 479.

[272] *Id.*

[273] *Id.*

[274] *See supra* note 46 and accompanying text.

[275] *See infra* notes 264-265 and accompanying text.

[276] *Doe*, 334 F. Supp. 2d at 479.

[277] *Id.* at 501.

[278] *See supra* Part III.C.1.

[279] *Doe*, 334 F. Supp. 2d at 479.

NSL implicates two distinct interests: the target's privacy interest in the personal content of the records, and Doe's possessory and property interest in the records themselves. Because the target had knowingly exposed the records to the public, he cannot exert any Fourth Amendment rights.

The more difficult question is whether Doe's actual possession of the records grants him greater rights than the target. But this seems inconsistent. If the target must rely on the government's self-restraint, because he has no reasonable expectation of privacy, how can Doe expect anything more? On one hand: the information has already been exposed, corporations have weaker Fourth Amendment rights, and the government has weighty national security interests. On the other hand, Doe has maintained and secured the records; he had obligations to its customers to maintain their privacy; and the Supreme Court has held that a corporation has the right to be free of unreasonable meddling, and that protection is already afforded by the requirement that any subpoena meet the *Walling* standards.

Overall, it seems that society expects the government to bear some burden before it can compel production of telecommunications records, rather than allowing the government to invade a corporation's possessory interests limited only by its own self-restraint. Administrative subpoena law thus recognizes certain minimal standards that the government must meet, and implies that a subpoenaed party has some Fourth Amendment interests, although the Supreme Court has never explicitly held as much.

Assuming that Doe can meet the threshold requirement of showing he has a Fourth Amendment interest, then the NSL was a reasonable search and seizure. First, it complied with the three *Walling* requirements. The purpose of the investigation was specifically authorized by statute; the documents were likely relevant to the investigation; and the documents were specifically described, limited only to the target's records held by the ISP. Second, although judicial review is not explicitly provided for in § 2709, it is implied not only by law but also by the facts of this case, because Doe in fact sought and received judicial review. Nor was Doe coerced into complying. The FBI simply sent a letter and waited for Doe's response. It did not dispatch special agents to seize the records or threaten Doe with arrest. The harsh tone of the letter and its failure to inform Doe that he could seek redress through the courts did not preclude judicial review.

The *Doe* court was right to be distressed about the government's power under § 2709. One concern is that the *Walling* requirements limit the court to asking if the investigation is authorized, and not if Congress properly granted the authority to investigate. As discussed earlier, this balancing has already been accomplished by the Court in specifying the *Walling* requirements; the Supreme Court presumes the agency's authority to investigate is proper. The *Doe* court's distress about § 2709 is futile in light of a Congress that grants broad agency power to subpoena and a Supreme Court that prescribes only nominal checks on that power. As the law stands, the FBI can issue an NSL and demand a wide variety of records upon mere self-certification.

The *Doe* court's concern about the possible "parade of horribles" caused by the government intruding into our personal records is justified, but perhaps overstated.[280] It said that NSLs pose the "gravest peril[] to personal liberties," and that it was incumbent upon the judiciary to "steer a principled course faithful and true to our still-honored founding values."[281] These same fears were raised before the Supreme Court seventy years ago.[282] There, petitioners were similarly concerned about the breadth of an administrative agency's subpoena powers, and likened the consequences to the infamous Star Chamber of the Stuarts.[283] Justice Cardozo's response, "Historians may find hyperbole in the sanguinary simile,"[284] seems as appropriate today as it was then.

[280] *Id.* at 478 (describing the need to carefully balance national security concerns with the protection of individual freedom and constitutional rights).

[281] *Id.*

[282] Jones v. SEC, 298 U.S. 1, 32-33 (1936) (Cardozo, J., dissenting) (describing the need to balance protection against abuses of government power with the need to grant agencies sufficient power to protect the public interest).

[283] *See supra* note 2.

[284] *Jones*, 298 U.S. at 33.