Fordham Urban Law Journal

Volume 33 | Number 5 Article 5

2006

"Special Delivery:" Where do National Security Letters Fit into the Fourth Amendment?

Lauren M. Weiner

"SPECIAL" DELIVERY: WHERE DO NATIONAL SECURITY LETTERS FIT INTO THE FOURTH AMENDMENT?

Lauren M. Weiner [*]

INTRODUCTION

In the summer of 2005, agents from the Federal Bureau of Investigation ("FBI") visited George Christian, a digital services manager for over three-dozen Connecticut libraries[1] and presented him with a "National Security Letter."[2] The letter directed Mr. Christian to turn over subscriber information and access logs of Internet users at a certain library.[3] Over 30,000 National Security Letters, or "NSLs," are issued each year, presumably to investigate terrorists.[4] But because NSLs require the recipient to keep the letter secret,[5] what do we really know about NSLs?

Historically, if an investigation concerned "international terrorist activities" it was subject to little oversight.[6] Serious abuses of investigative power, however, led Congress to enact legislation designed to protect civil liberties, even for "foreign intelligence investigations."[7] After the terrorist

[*] J.D. candidate, Fordham University School of Law, 2007; B.S., Northwestern University, 2000. I would like to thank Professor Dan Richman for his guidance, Genevive Blake for her careful edits and Nick Mitchell for thoughtfully reviewing countless drafts and helping me clarify my position on this issue.

1. Barton Gellman, *The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, WASH. POST, Nov. 6, 2005, at A1. Under the newest changes to the USA PATRIOT Act, most libraries are now exempt from complying with NSLs. *See* David Stout, *Bush Signs Bill Renewing Patriot Act*, N.Y. TIMES, Mar. 9, 2006 (online edition, *available at* http://www.nytimes.com/2006/03/09/politics/09cnd-patriot.html).

2. Gellman, *supra* note 1, at A1.

3. *Id.*

4. *Id.*

5. *See* 18 U.S.C. § 2709(c) (2006).

6. Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215*, 1 J. NAT'L SECURITY L. & POL'Y 37, 39-40 (2005).

7. Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871 (2006).

attacks of September 11, 2001 ("9/11"), Congress passed the USA PATRIOT Act ("PATRIOT Act")[8] to aid law enforcement efforts to fight terrorism.[9] The PATRIOT Act broadened the scope of certain investigatory tools, making the job of law enforcement easier and subjecting law enforcement agencies to fewer limitations. One such tool, National Security Letters, gives the government the authority to request certain types of transactional records without requiring judicial pre-approval and without giving the recipient a meaningful method to challenge it.[10] This begs the question: what does it mean to "fight terrorism?" Is the goal to prevent further terrorist attacks or to prosecute the perpetrators? That question has some important implications as the government struggles to sculpt a regulatory regime for terrorism cases that will be both effective and constitutional. There are different rules and procedures for domestic criminal investigations than for investigations that focus on foreign intelligence gathering. It is clear that a murder investigation is intended to gather evidence that will lead to the prosecution of the killer. When it comes to counter-terrorism, however, it is not as easy to determine whether the investigation is for the purpose of deterrence or prosecution. Furthermore, what safeguard is there to prevent a law enforcement officer, even one with good intentions, from using the less stringent standards for foreign intelligence operations to gather evidence that wouldn't otherwise be accessible if he had to follow the stricter procedures for a domestic criminal investigation?

In several of its sections, the PATRIOT Act combines the procedures for traditional criminal law enforcement with the looser procedural standards that are in place for foreign counterintelligence investigations.[11] In some respects, NSLs are similar to administrative subpoenas—an information-gathering tool for domestic criminal investigations. In fact, the Bush Administration has suggested granting the FBI administrative subpoena power for counter-terrorism investigations so they would have the same tools available to catch terrorists as are already available to catch doctors

8. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 15, 18, 22, 31, 42, 49 and 50 U.S.C. (2006)).

9. Neil A. Lewis & Robert Pear, *A Nation Challenged: Congress; Negotiators Back Scaled-Down Bill to Battle Terror*, N.Y. TIMES, Oct. 2, 2001, at A1.

10. Woods, *supra* note 6, at 41. NSLs were not created by the PATRIOT Act, but it expanded the government's power to use them. *See infra* notes 14-18 and accompanying text.

11. See *infra* notes 73-96 and accompanying text for a discussion of foreign intelligence investigations.

engaged in insurance fraud.[12] This suggestion, however, over-simplifies the issue and disregards the fundamental differences between foreign intelligence investigations and criminal investigations—especially as related to the constitutionality of warrantless searches.

So what are NSLs? Are they ordinary domestic law enforcement tools that have the looser standards of foreign intelligence-gathering tools? Or are they tools for foreign intelligence that may be used for ordinary domestic criminal investigations? Are they constitutional? And even if constitutional, are they still problematic?

This Comment will examine NSLs both in the context of foreign intelligence and domestic criminal investigations. There are substantial arguments on both sides of the debate over the constitutionality of NSLs; this Comment will primarily be focused on how to classify NSLs and how to use them in a manner that reduces the potential for abuse or over-reaching. This Comment will argue that NSLs are not foreign intelligence tools, but are merely foreign intelligence exceptions to domestic laws that allow law enforcement access to records that would otherwise be protected by privacy laws. Accordingly, NSLs must be able to satisfy the constitutional requirements for domestic searches. First, this Comment will provide background on NSLs, the Fourth Amendment, and the Foreign Intelligence Surveillance Act. Then, this Comment will examine NSLs in the context of the permissible exceptions to the warrant requirement for searches—specifically the "special needs" exception. Finally, this Comment will argue that even if NSLs are constitutional despite their issuance without a warrant, they still have great potential for abuse and additional safeguards beyond the recent revisions are necessary.

PART I: BACKGROUND

In evaluating laws pertaining to criminal procedure, one must make a distinction between investigations focused on "foreign agents," or general foreign intelligence, and ordinary domestic criminal investigations.[13] Law enforcement officials are authorized to use a more expansive set of tools to obtain records and information when the investigation pertains to foreign persons or intelligence activities. This section will first examine the statutes authorizing NSLs, and will outline their powers and their

12. *See* President George W. Bush, Remarks by the President in a Conversation on the U.S.A. Patriot Act (April 20, 2004), *available at* http://www.vote-smart.org/speech_detail.php?speech_id=33849 (last visited February 25, 2006); *see also* David E. Sanger, *Two Years Later: The President; President Urging Wider U.S. Powers in Terrorism Law*, N.Y. TIMES, Sept. 11, 2003, at A1.

13. *See infra* notes 73-96 and accompanying text.

limitations. This section will also discuss the Fourth Amendment and its relationship to domestic and foreign investigations because, in some respects, NSLs are a hybrid of foreign and domestic investigatory standards.

A. National Security Letters

Law enforcement officials are authorized to issue NSLs under three statutes: the Electronic Communications Privacy Act of 1986 ("ECPA"),[14] the Right to Financial Privacy Act,[15] and the Fair Credit Reporting Act.[16] These statutes were enacted to offer protection to individuals for records in the possession of third parties, an area not covered by the Fourth Amendment.[17] NSLs were included as an exception to this protection by allowing access to these records for government agencies "authorized to conduct foreign counter- or foreign positive-intelligence activities."[18]

This Note will primarily focus on the ECPA—the statute that has most frequently been evaluated in the context of national security.[19] The ECPA was designed to give statutory protection to stored electronic information held by a "wire or electronic communications service provider."[20]

Section 2709, the national security provision of Title II of the ECPA, was designed to enable law enforcement to investigate suspected terrorists or foreign agents.[21] The original version of the ECPA section 2709 allowed the FBI to compel production of (1) subscriber information (limited to name, address, and length of service); (2) local and long

14. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

15. 12 U.S.C. § 3414(a)(5)(A) (Supp. 2004).

16. 15 U.S.C. §§ 1681u, 1681v (Supp. 2004). Another statute, 50 U.S.C. § 436(b) (2006), authorizes the government to compel disclosure of certain records of current or former government employees who at one time had access to classified information.

17. Woods, *supra* note 6, at 46-49. The Supreme Court's holding in *United States v. Miller* permitted the government to access financial records from a bank without violating the Fourth Amendment. *See* 425 U.S. 435, 444 (1976).

18. Woods, *supra* note 6, at 43.

19. Much of the uproar over NSLs centered on their use to obtain library records. For a detailed discussion see generally Susan Nevelow Mart, *Protecting the Lady from Toledo: Post-USA PATRIOT Act Electronic Surveillance at the Library*, 96 L. LIBR. J. 449 (2004). Librarians and others raised concerns that library patrons may believe that the FBI is looking into the books they read and the websites they visit on library computers. *Id.* at 468.

20. Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1867 (2006) (codified as amended at 18 U.S.C. § 2709). Title I of the statute defines an electronic communications service ("ECS") as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (2002).

21. Title II is also referred to as the "Stored Wire and Electronic Communications and Transactional Records Act." *See* Pub. L. No. 99-508, § 201.

distance toll billing records; and (3) electronic communication transactional records.[22]

The standard for obtaining this information under the original version of the ECPA was that the information sought had to be "relevant to an authorized foreign counterintelligence investigation," and there had to be "specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertain[ed] [was] a foreign power or agent of a foreign power."[23] There are other provisions of Title II of the ECPA that allow law enforcement to obtain similar types of information in the context of a "criminal investigation," but, unlike NSLs, those provisions require judicial pre-approval.[24] The fact that the ECPA provides access to records in domestic criminal investigations may be a significant factor in evaluating whether NSLs under section 2709 serve a purpose beyond the need for ordinary law enforcement.[25]

Further, while domestic criminal investigations require the approval of a judge, NSLs for national security investigations are authorized by the agency that issues them.[26] Before passage of the PATRIOT Act, an NSL required only the approval of an FBI official with a rank "not lower than Deputy Assistant Director."[27] The issues of self-authorization and rank of law enforcement officials authorized to approve NSLs will be revisited in later sections of this Note, as part of a discussion of the potential for overreaching on the part of the law enforcement agencies.[28]

Section 2709 remained relatively unchanged[29] until the USA PATRIOT

22. Memorandum from General Counsel, Fed. Bureau of Investigation to All Field Offices 2 (Nov. 28, 2001) [hereinafter FBI NSL Memo]; *see also* H.R. REP. NO. 103-46, at 6 (1993), *reprinted in* 1993 U.S.C.C.A.N. 1913, 1917. "Transactional records" generally refer to records of the communication that do not reveal their content. For example, a transactional record would reveal the phone numbers dialed from a particular phone, but would not reveal the substance of the calls. *See* FBI NSL Memo, *supra*, at 4-5.

23. 18 U.S.C. § 2709 (1996).

24. 18 U.S.C. § 2703(a) (2006) (requiring a warrant); 18 U.S.C. § 2703(b)(1)(B)(i) (requiring a subpoena); 18 U.S.C. § 2703(d) (requiring a court order).

25. See *infra* notes 125-45 and accompanying text for a discussion of the "special needs" exception to the Fourth Amendment.

26. 18 U.S.C. §§ 2709(b)(1)-(2).

27. *Id.* Other sections of Title II require the FBI to obtain a warrant or a subpoena, but these sections pertain to "criminal investigation[s]," not foreign intelligence. *See* 18 U.S.C. §§ 2703 (a), (b)(1)(B)(i), (d). See also *infra* notes 97-118 and accompanying text for a further discussion of domestic criminal investigations.

28. *See infra* note 39 and accompanying text.

29. In 1993, following the first World Trade Center bombings, the "foreign power" requirement was loosened to allow investigation of an individual who communicated with a foreign power regarding terrorism or foreign intelligence. 18 U.S.C. § 2709 (1994); H.R. REP. NO. 103-46, at 3 (1993).

Act enlarged NSL power specifically, and foreign intelligence-gathering power more generally. Passed seven weeks after 9/11, the draft bill of the USA PATRIOT Act[30] called for, in pertinent part, expansion of the government's information-gathering powers by eliminating or reducing judicial oversight.[31] A period of intense negotiations between the legislative and executive branches followed.[32] The proposal by Senator Patrick Leahy would have allowed increased intelligence powers, but would have included significantly more judicial supervision than the administration's plan.[33] The Bush administration made it clear that its priority was to get new anti-terrorism legislation through Congress as quickly as possible.[34] While congressional democrats, like Senator Leahy, indicated that Congress would not be pushed to act in haste and that they would continue to work to balance law enforcement needs with constitutional rights,[35] many of the negotiations were done behind closed doors in private meetings. Senator Russ Feingold stated "there has not been an open process in the Judiciary Committee, much less the full Senate, for Senators to have an opportunity to raise concerns about how far this bill goes in giving power to law enforcement to . . . investigate law-abiding U.S. citizens."[36] Regardless of such concerns, the PATRIOT Act was passed and on October 26, 2001, it was signed into law.[37]

The PATRIOT Act changed NSLs by expanding the FBI's power to use them and by codifying and correcting disparities in pre-existing law

30. *See generally* Consultation and Discussion Draft Bill to Combat Terrorism and Defend the Nation Against Terrorist Acts, and for Other Purposes, with the short title, "Anti-Terrorism Act of 2001" (administration draft bill, Sept. 19, 2001), *available at* www.epic.org/privacy/terrorism/ata2001_text.pdf (last visited Sept. 25, 2006); *see also* Beryl A. Howell, *Seven Weeks: the Making of the U.S.A. PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1153 n.43 (2004). The administration's draft bill was renamed because the initials "ATA" were too close to the name of one of the 9/11 hijackers, Mohamed Atta. Howell, *supra*, at 1153 n.43.

31. Howell, *supra* note 30, at 1146-54.

32. *Id.* at 1154.

33. *See generally* Draft, Uniting and Strengthening America Act (Senator Leahy's draft bill), *available at* http://leahy.senate.gov/press/200109/AYO01_714.pdf (last visited Oct. 20, 2006). Leahy's plan, for example, allowed the information from a grand jury investigation to be shared, but required court authorization and a certification that the matters were relevant to a terrorism investigation. *Id.* at 130-31.

34. *See* Howell, *supra* note 30, at 1160-62 (discussing the administration's comments regarding the passage of the legislation).

35. *See* 147 CONG. REC. S10, 547 (daily ed. Oct. 11, 2001).

36. 147 CONG. REC. S10, 36301 (daily ed. Oct. 9, 2001).

37. Pub. L. No. 107-56, 115 Stat. 272 (2001). While certain provisions of the PATRIOT Act were originally scheduled to "sunset" on December 31, 2005, negotiations continued past the deadline and the reauthorization of the Act was signed into law on March 9, 2006. *See* Stout, *supra* note 1.

relating to Internet and telephone records gathering.[38] NSLs were broadened by (1) expanding the scope of applicable investigations from "authorized foreign counterintelligence operation[s]" to "authorized investigation[s] to protect against international terrorism or clandestine intelligence activities"; (2) compelling production where the information sought is merely "relevant" to the investigation; (3) substituting relevance for "specific and articulable facts"; and (4) lowering the rank of the FBI official who can authorize an NSL from "Deputy Assistant Director," to "Special Agent in Charge" of a field office.[39]

B. The Fourth Amendment

Much of the debate surrounding law enforcement power involves the Fourth Amendment and whether or not certain law enforcement tools are violative of the rights it guarantees. The Fourth Amendment provides that the

> right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[40]

In order for the Fourth Amendment to effectively regulate the investigatory process, it needs to have a "meaningful enforcement mechanism" and must be broadly applicable.[41]

The Fourth Amendment will protect individuals from the abuse of law enforcement power if the contested activity is classifiable as a "search" or a "seizure."[42] The Supreme Court has held that a seizure is a "meaningful

38. *See, e.g.*, Pub. L. No. 107-56, § 209, 115 Stat. at 283 (correcting the disparate requirements to allow access to stored e-mail and voicemail).

39. *See* 18 U.S.C. § 2709 (2006). There are only a limited number of Deputy Assistant Directors, located at FBI headquarters and in the New York and Los Angeles field offices. There are fifty-six FBI field offices in the United States and each of those, with the exception of the New York and Los Angeles offices, have one Special Agent in Charge ("SAC"). The New York and Los Angeles offices have SACs for special projects or divisions. The head of the New York and Los Angeles field offices are Assistant Directors. *See* Fed. Bureau of Investigation, Your Local FBI Office Field Divisions, *http://www.fbi.gov/contact/fo/fo.htm* (last visited Sept. 25, 2006).

40. U.S. CONST. amend. IV.

41. Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 749-50 (2005). Applicability refers to the specific law enforcement activities that are covered by the Fourth Amendment. *Id.*

42. WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1 (4th ed. 2004) (citing Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 356 (1974)) [hereinafter LAFAVE, SEARCH AND SEIZURE]; *see also*

interference with an individual's possessory interests" in property.[43] The definition of a search is less clear and has been frequently reevaluated.[44] Taken as a whole, it seems that searches are physical intrusions into "a constitutionally protected area."[45] If the intrusion is classified as either a search or seizure, it must be "reasonable."[46]

One way for law enforcement to conduct a "reasonable" search is to obtain a warrant.[47] The Supreme Court has expressed its preference for searches made with judicial pre-approval, rather than having search and seizure decisions made on the scene by police officers.[48] In order for a warrant to be granted, there must be a showing of "probable cause."[49] Probable cause requires law enforcement officers to have sufficient evidence to convince a neutral magistrate that the search is likely to reveal criminal activity.[50] Search warrants may not be used in cases of mere suspicion, because they require a showing of facts to support probable cause.[51]

A search where the law enforcement officer has first obtained a warrant is presumptively reasonable, but there are circumstances in which the Fourth Amendment permits searches without one.[52] Generally speaking, an activity covered by the Fourth Amendment (i.e. a search or seizure) must be reasonable; if it is not covered then there are no limitations on law

Solove, *supra* note 41, at 750.

43. LAFAVE, SEARCH AND SEIZURE, *supra* note 42, § 2.1(a) (citations omitted).

44. *Id.*

45. *Id.* (citing Silverman v. United States, 365 U.S. 505 (1961)).

46. *See* Solove, *supra* note 41, at 750.

47. For a detailed discussion of the history of the warrant clause see Harold J. Krent, *The Continuity Principle, Administrative Constraint, and the Fourth Amendment*, 81 NOTRE DAME L. REV. 53, 57-61 (2005).

48. LAFAVE, SEARCH AND SEIZURE, *supra* note 42, § 4.1 (citations omitted). See *infra* note 152 for a discussion of potential abuse of power when decisions are in the hands of low-level officers.

49. U.S. CONST. amend. IV. The probable cause requirement was included in the Fourth Amendment to protect individuals from indiscriminate government searches and seizures. *See generally* Ronald M. Gould & Simon Stern, *Catastrophic Threats and the Fourth Amendment*, 77 S. CAL. L. REV. 777, 786 (2004). The Framers of the Constitution included the probable cause requirement as part of the Bill of Rights in reaction to the arbitrary abuses of police power suffered under British rule, especially warrants that did not specifically name an individual suspect. *Id.* at 790.

50. Katz v. United States, 389 U.S. 347, 357 (1967).

51. U.S. CONST. amend. IV (requiring law enforcement officers requesting a search warrant to "particularly describ[e] the place to be searched, and the persons or things to be seized").

52. Solove, *supra* note 41, at 751-53 (discussing the retreat of Fourth Amendment protections). For a discussion of warrantless searches see *infra* notes 71-72 and accompanying text.

enforcement's power under the Fourth Amendment.[53]

While much Fourth Amendment jurisprudence regarding the applicability of the Fourth Amendment relies upon Justice Harlan's concurrence in *Katz v. United States*,[54] there has been much debate and dissension over the definition of "privacy."[55] According to Justice Harlan, the Fourth Amendment is applicable if the individual has an "actual" (subjective) expectation of privacy, and that expectation is "one that society is prepared to recognize as reasonable."[56] Prior to the Court's holding in *Katz*, an intrusion into an individual's privacy required an actual physical invasion of an individual's home or person.[57] While the holding in *Katz* effectively rejected this conception of privacy,[58] there are other views of privacy that are equally, if not more, limiting to the scope of Fourth Amendment protection. Professor Daniel Solove refers to one such conception as the "secrecy paradigm"—that the only invasion of privacy occurs when a "deep secret is uncovered."[59] According to this view, records, such as the transactional records accessible by issuing an NSL, would not be considered "secret" enough to be private and thus would not be covered by the Fourth Amendment.[60]

An additional limitation on the Fourth Amendment's applicability pertaining to NSLs is the "third party doctrine." The third party doctrine provides that information placed in the hands of, or that is known to, a third party, no longer falls under a reasonable expectation of privacy.[61] Examples include bank records[62] and records of the phone numbers that a person dials.[63] The third party doctrine conceivably applies to the records accessible by an NSL; subscriber information and toll records are in the

53. Solove, *supra* note 41, at 750.

54. 389 U.S. at 360 (Harlan, J., concurring).

55. Solove, *supra* note 41, at 751.

56. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (internal quotations omitted).

57. *See generally* Olmstead v. United States, 277 U.S. 438 (1928) (holding that an individual was not protected from government wiretapping because the government did not physically enter his home).

58. *Katz*, 389 U.S. at 351 (holding that the Fourth Amendment "protects people, not places").

59. *See* Solove, *supra* note 41, at 751 (citing DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 42 (2004)).

60. *Id.* at 752-53.

61. *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.").

62. *Id.* at 441-43.

63. *See* Smith v. Maryland, 442 U.S. 735 (1979). In *Smith*, the Court held that because people are aware that the numbers they dial go to the phone company, they do not "harbor any general expectation that the numbers they dial will remain secret." *Id.* at 743.

possession of the phone company or Internet service provider ("ISP").

While the primary remedy for a violation of the Fourth Amendment is the exclusionary rule,[64] searches made pursuant to a warrant may be challenged only after they are executed.[65] It may be difficult to suppress evidence gathered from a search executed pursuant to a warrant, however, as the courts tend to find that the search warrant was presumptively valid if signed by a neutral magistrate.[66]

In the context of NSLs, it is important to note that third parties, such as a telephone company, lack standing to challenge the validity of a search, even if it affects the third party's privacy interests.[67] A third party has its own Fourth Amendment right to freedom from unreasonable search and seizure; it cannot be required to turn over records absent consent or a Fourth Amendment sanctioned procedure.[68] For example, a subscriber to an Internet service would not be able to challenge a search of the records of the ISP; the provider would be the only party with the ability to challenge that search. Further, using search warrants as a means of obtaining information from a third party may be unnecessarily intrusive where the third party is willing to surrender the documents without compelling their production.[69]

Despite the preference for searches pursuant to a warrant from a constitutional perspective, there are arguments to be made against a warrant requirement. The process of obtaining a warrant requires a considerable expenditure of time—on the part of the judges who must examine the facts and the officers who must demonstrate the existence of probable cause with a showing of particular facts.[70] Accordingly, the Supreme Court has

64. The exclusionary rule allows the suppression of evidence obtained through a search that infringes upon an individual's Fourth Amendment rights. *See* United States v. Caladra, 414 U.S. 338 (1974); Weeks v. United States, 232 U.S. 383 (1914).

65. LAFAVE, SEARCH AND SEIZURE, *supra* note 42, § 4.1(f).

66. *Id.* § 11.2(b).

67. *Id.* § 11.3(d) (citing United States v. Miller, 425 U.S. 435 *passim* (1976) (holding bank customer could not challenge seizure of records from the bank)).

68. *E.g.*, Seattle Times News Servs., *Phone Records: Telecoms May Be in Trouble*, SEATTLE TIMES, May 13, 2006, at A1.

69. *See* Graham Hughes, *Administrative Subpoenas and the Grand Jury: Converging Streams of Criminal and Civil Compulsory Process*, 47 VAND. L. REV. 573, 575 (1994). Search warrants offer Fourth Amendment protections that may not be necessary when dealing with third parties, such as telephone carriers, who might be willing to turn over the requested information on demand. *See generally* United States v. Miller, 425 U.S. 435 (1976). Department of Justice policy advises that warrants should not be used in an investigation if the information sought can be obtained through less intrusive means. 28 C.F.R. § 59.1 (2005); *see also* FBI NSL Memo, *supra* note 22, at 3.

70. *See* Krent, *supra* note 47, at 62 ("The Framers' decision to require ex ante review in each case reflects their commitment not to relegate protection for privacy to after-the-fact

enumerated two tests applied by courts to determine when a warrantless search will overcome the presumption of unreasonableness. The "special-needs" exception allows warrantless searches where the primary purpose in administering the search goes beyond the ordinary need for law enforcement and the state's interest in that purpose outweighs the individual's privacy interest.[71] The other test, called the "reasonableness balancing test," permits warrantless searches where the totality of the state's legitimate interests outweigh the privacy interests of the individual to be searched.[72] Both tests are potentially applicable to NSLs, which, after all, are searches performed without judicial review.

1. Foreign Intelligence Investigations

This section, along with a discussion of information-gathering for domestic investigations,[73] will provide context in which to determine whether NSLs fall within the realm of foreign intelligence—and accordingly should be placed under the auspices of the specialized court that handles foreign intelligence matters—or if they are actually tools for ordinary domestic law enforcement. Although discussion of foreign intelligence law centers on the regulations for surveillance and wiretaps, it is applicable to NSLs both because foreign intelligence law now includes access to "tangible objects," and because the standards set forth under foreign intelligence law are similar to those in section 2709 of the ECPA.[74]

Intelligence-gathering for domestic criminal investigations clearly falls under the auspices of the Fourth Amendment.[75] Nevertheless, the question of how to regulate national security intelligence remained open for many years. In 1972, the Supreme Court, in *United States v. U.S. Dist. Court*, commonly known as the "Keith" case, found that the restrictions placed on wiretaps for domestic investigations did not limit "the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means."[76] The Court further held that "*security* surveillance may

mechanisms . . . .").

71. *See* Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (quoting New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring)).

72. *See* United States v. Knights, 534 U.S. 112, 118-19 (2001); s*ee also* Wyoming v. Houghton, 526 U.S. 295, 300 (1999); Bell v. Wolfish, 441 U.S. 520, 559 (1979).

73. *See infra* notes 97-118 and accompanying text.

74. *See supra* note 26.

75. *See* Solove, *supra* note 41, at 754-56. Wiretapping is covered by the Fourth Amendment, but is regulated through the Wiretap Act. *Id.*; *see also* 18 U.S.C. §§ 2510-2520 (2000).

76. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 307-08 (1972).

involve different policy and practical considerations from the surveillance of *ordinary* crime."[77] The Court declined, however, to rule on the executive's power to use surveillance "with respect to the activities of foreign powers, within or without this country."[78] The decision in *Keith* indicated that the Supreme Court accepted the possibility that "[d]ifferent standards," other than a traditional warrant, "may be compatible with the Fourth Amendment if [it is] reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[79]

Six years after the decision in *Keith*, Congress addressed the questions left unanswered by its holding.[80] The Foreign Intelligence Surveillance Act ("FISA") of 1978[81] was enacted by Congress to create a regulatory regime outside of the traditional regime for criminal law, which would act as a check on the executive's power to conduct investigations of "foreign agents" in the United States.[82] Under FISA, the government must apply for orders from the Foreign Intelligence Surveillance Court ("FISC") in order to conduct intelligence-gathering activities.[83] The FISC is designed to hear requests for court orders that pertain to foreign intelligence.[84]

Pre-PATRIOT Act, FISA orders were primarily used for electronic surveillance of foreign agents.[85] Section 215 of the PATRIOT Act

77. *Id.* at 322 (internal quotations omitted) (emphasis added).

78. *Id.* at 307-08. The *Keith* Court also addressed the question of the Fourth Amendment implications of national security surveillance without the prior approval of a neutral magistrate, as would be required to obtain a Title III wiretap order. *See* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1315 (2004) (citing *Keith*, 407 U.S. at 309 (citations omitted)).

79. *Keith*, 407 U.S. at 322.

80. *See* Richard Henry Seamon & William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319, 321 (2005); Solove, *supra* note 41, at 756.

81. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified at 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871).

82. Swire, *supra* note 78, at 1313.

83. *See* 50 U.S.C. § 1803 (2006). For surveillance activities involving communications "exclusively between or among foreign powers" with "no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party," the government may conduct the surveillance without a court order. *See* 50 U.S.C. § 1802 (a)(1).

84. *See* 50 U.S.C. § 1803. The FISC currently consists of eleven district court judges appointed by the Chief Justice of the Supreme Court. *Id.* Originally, the FISC had seven judges, but the PATRIOT Act added additional judges. *See* USA PATRIOT Act, Pub. L. No. 107-56, § 208(i), 115 Stat. 272, 283 (2001).

85. Following the bombings in Oklahoma City and the World Trade Center, Congress authorized FISA orders for travel records. *See* 50 U.S.C. §§ 1861-1862 (2006) (allowing access to records held by common carriers (airlines, trains, etc.), physical storage facilities

amended FISA, however, by allowing its use to compel production of business records and other "tangible objects."[86] The scope of materials covered by section 215 now includes books, records, papers, documents, and "other items," provided that the government can make the requisite showing to the FISC.[87]

Prior to the passage of the PATRIOT Act, the showing required for a FISA order was probable cause that the target of the request was a "foreign power or an agent of a foreign power" and that the "purpose" of the investigation was to gather foreign intelligence.[88] Now, FISA's scope has been expanded to include investigations where foreign intelligence gathering is a "*significant* purpose."[89] The PATRIOT Act also lowered the burden of proof for the government to obtain an order for business records or for other "tangible things."[90] Previously, a FISA order required a showing of "specific and articulable facts" giving "reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power."[91] Now, when applying for a FISA order, the application need only "specify that the records concerned are sought for an authorized investigation."[92] The Department of Justice ("DOJ") has the discretion to define the term "authorized investigation."[93] Moreover, FISA orders now can be used to investigate virtually anyone, as there is no requirement that the request include a specific target.[94] The investigation must simply "protect against international terrorism or clandestine intelligence activities" —a broad standard that could include many types of investigations.[95] The implications of this change are potentially enormous—it allows the government to use a FISA order to gather information for an ordinary domestic prosecution if one of the purposes of the investigation relates to foreign intelligence.[96]

(rental lockers, etc.), public accommodation facilities (hotels, etc.), and vehicle rental facilities).

86. *See* Swire, *supra* note 78, at 1331.

87. *See* 50 U.S.C.A. § 1861(b)(2) (West 2003).

88. 50 U.S.C. § 1805(a)(3)(A) (2000).

89. *Id.* § 1804(a)(7)(B), *amended by* USA PATRIOT Act § 204 (emphasis added); *see also* Solove, *supra* note 41, at 757.

90. USA PATRIOT Act § 215.

91. 50 U.S.C. § 1861(b)(2)(B) (1998). *Compare* U.S. CONST. amend. IV.

92. 50 U.S.C.A § 1861(b)(2) (West 2006).

93. Swire, *supra* note 78, at 1331; *see also* FBI NSL Memo, *supra* note 22, at 2-3.

94. *See* Swire, *supra* note 78, at 1331.

95. 50 U.S.C.A. §1861(b)(2) (West 2006).

96. *See, e.g.*, Solove, *supra* note 41, at 757.

2. Domestic Law Enforcement

In a previous section, this Note established that NSLs were originally intended as foreign intelligence exceptions to statutes that protect privacy.[97] Given that NSLs are not subject to restraints placed on other foreign intelligence investigations through FISA,[98] e.g., pre-approval by the FISC, arguably, NSLs should then be subjected to either the constitutional or statutory protections required for domestic criminal investigations. This next section will briefly examine two types of information-gathering techniques for criminal investigations: administrative subpoenas and grand jury subpoenas. These tools do not violate the Fourth Amendment, despite procedures that differ from ordinary search warrants. Accordingly, they may serve as a valuable comparison when deciding whether NSLs are constitutional under the Fourth Amendment.

a. Administrative Subpoenas

Administrative subpoenas are issued by federal agencies pursuant to a delegation of power from Congress.[99] An administrative subpoena can compel documents and testimony.[100] Administrative subpoenas also enable investigators to bypass the Fourth Amendment's probable cause requirement in criminal investigations.[101] An administrative subpoena

97. *See supra* Part I.A and accompanying text.

98. *See supra* Part I.A and accompanying text.

99. *See* Katherine Scherb, Comment, *Administrative Subpoenas for Private Financial Records: What Protection for Privacy Does the Fourth Amendment Afford?*, 1996 WIS. L. REV. 1075, 1076-85 (providing a history of the development of administrative subpoena power). Examples of agencies that issue administrative subpoenas include the Securities and Exchange Commission ("SEC") and the Internal Revenue Service ("IRS"). *See* 15 U.S.C. § 78u(b) (2002) (investigating violations of securities law); 26 U.S.C. § 7602(a) (1998) (investigating tax code violations); *see also* Health Insurance Portability and Accountability Act of 1996 (HIPPA), 18 U.S.C. § 3486 (2000). The Attorney General was granted the power to conduct criminal investigations into healthcare fraud using a civil administrative subpoena. 18 U.S.C. § 3486.

100. *See* Risa Berkower, Note, *Sliding Down a Slippery Slope? The Future Use of Administrative Subpoenas in Criminal Investigations*, 73 FORDHAM L. REV. 2251, 2257 (2005).

101. *See* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946) (holding that compliance with an administrative subpoena did not present a question of an actual search or seizure and, accordingly, the Fourth Amendment was not directly applicable); *see also* Berkower, *supra* note 100, at 2253 (citing Doe v. United States, 253 F.3d 256, 263 (6th Cir. 2001) (holding that no probable cause is required to issue an administrative subpoena under 18 U.S.C. § 3486)). Courts treat civil and criminal matters differently for Fourth Amendment purposes; the Constitution is far more protective of a criminal defendant's rights. *See* Berkower, *supra* note 100 at 2261 (citing Ronald F. Wright, Note, *The Civil and*

initiates an open proceeding with plenty of opportunity for a party opposing the requested materials to challenge the subpoena in court. Furthermore, the Supreme Court has indicated that administrative subpoenas are not actual searches and as such, need not require a showing of probable cause.[102] Generally, administrative subpoenas will be enforced by the courts so long as: (1) the investigation has a legitimate purpose; (2) the inquiry is related to that purpose; (3) the agency does not already have the information sought; and (4) the agency follows proper procedures.[103] Administrative subpoenas "commence[] an adversar[ial] process" that permits judicial review of its reasonableness.[104]

b. Grand Jury Subpoenas

The federal grand jury is an investigative body given broad power to compel testimony and production of documents.[105] An investigative grand jury has the authority, absent a showing of valid privilege, to subpoena any books, papers, documents, data, or other objects,[106] and to compel witness testimony.[107] A grand jury subpoena may be issued without a showing of probable cause,[108] and the grand jury "can investigate merely on suspicion that the law is being violated, or even just because it wants assurance that it is not."[109]

One limitation on the grand jury subpoena power is Rule 17(c) of the Federal Rules of Criminal Procedure, which provides that, "on motion made promptly, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive."[110] It is, however, exceedingly difficult to quash a subpoena once it is issued.[111] The moving party must

Criminal Methodologies of the Fourth Amendment, 93 YALE L.J. 1127, 1127 (1984)).

102. *See, e.g.*, *Okla. Press Publ'g Co.*, 327 U.S. at 209.

103. *See* Doe v. United States, 334 F. Supp. 2d 471, 485 (S.D.N.Y. 2004) (citing United States v. Powell, 379 U.S. 48, 57-58 (1964)).

104. *See* United States v. Bailey, 228 F.3d 341, 348 (4th Cir. 2000) ("As judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from, that process.").

105. *See* Sara Sun Beale & James E. Felman, *The Consequences of Enlisting Federal Grand Juries in the War on Terrorism: Assessing the USA PATRIOT Act's Changes to Grand Jury Secrecy*, 25 HARV. J.L. & PUB. POL'Y 699, 700 (2002).

106. *See id.* at 701.

107. *See id.* A witness may refuse to speak to an investigator, but is not equally free to refuse to testify before the grand jury. *Id.*

108. *Id.* at 701-02.

109. United States v. Morton Salt Co., 338 U.S. 632, 642-43 (1950).

110. FED. R. CRIM. P. 17(c); *see also* United States v. R. Enters., Inc., 498 U.S. 292, 298-99 (1991) (internal citations omitted).

111. *See generally R. Enters., Inc.*, 498 U.S. 292.

show that the subpoena is "unreasonable or oppressive," and that the motion will fail if there is a "reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation."[112]

An individual subpoenaed by a grand jury cannot directly challenge the subpoena; the individual must refuse to comply and, if the government initiates a contempt proceeding, can then assert that the subpoena is unreasonably burdensome.[113] A target[114] of a grand jury investigation can assert that the subpoenaed documents (or testimony) falls under a valid constitutional,[115] statutory,[116] or common law[117] privilege, even if those documents are in the possession of a third party.[118]

PART II. NSLS AND DOMESTIC CRIMINAL INVESTIGATIONS

Thus far, this Note has discussed the statutory framework of NSLs and then examined foreign intelligence and domestic criminal investigatory regimes in order to classify NSLs as belonging to one or the other. Prior to the passage of the PATRIOT Act and the loosening of the standards for issuing an NSL, it was easier to categorize NSLs as foreign intelligence tools. And as foreign intelligence tools, NSLs are not required to meet the standards for criminal investigations.[119] Now that NSLs can be used for investigations that have purposes besides foreign intelligence, perhaps NSLs should be required to satisfy the requirements for domestic criminal investigations. Because information regarding NSL use is classified, it is difficult to know if they are in fact being used to investigate. The potential for abuse alone, however, lends weight to the argument that NSLs must fit within a Fourth Amendment sanctioned regulatory regime for domestic criminal investigations.

112. *Id.* at 299-301 (citing United States v. Nixon, 418 U.S. 683, 700 (1974)).

113. *See* United States v. Ryan, 402 U.S. 530, 532 (1971) ("If . . . the subpoena is unduly burdensome or otherwise unlawful, [the recipient] may refuse to comply and litigate those questions in the event that contempt or similar proceedings are brought against him.").

114. Generally, there are three categories of individuals called before a grand jury: targets, subjects, and witnesses. *See* U.S. DEPT. OF JUSTICE, U.S. ATTORNEY'S MANUAL, CRIMINAL DIVISION § 9-11.151 (2006).

115. U.S. CONST. amends. I, V.

116. *See, e.g.*, 18 U.S.C. § 2515 (2000) (declaring that illegally obtained wiretap evidence cannot be introduced to the grand jury).

117. One example of a common law privilege is that between attorneys and clients. *See, e.g.*, Maine v. U.S. Dept. of the Interior, 298 F.3d 60, 71 (1st Cir. 2002).

118. *See Thirty-Second Annual Review of Criminal Procedure II. Preliminary Proceedings, Grand Jury*, 91 GEO. L.J. 210, 220-21 (citing Perlman v. United States, 247 U.S. 7, 12-13 (1918)).

119. *See* 18 U.S.C. § 2709 (2006) (stating requirements for issue of an NSL).

To effectively evaluate NSLs in the context of domestic criminal investigations, several things must first be established. First, does issuing an NSL constitute a search? If not, the use of NSLs need only be reasonable to satisfy the Fourth Amendment.[120] The FBI asserts that NSLs are not "searches" because they are only requests for information and recipients are not compelled to comply as NSLs are not backed with the contempt authority of the court.[121] While technically speaking the FBI's view is true, the average NSL recipient may nonetheless believe that a "search" is taking place.

Second, NSLs are issued without a warrant or any type of judicial order, such as a FISA order; they are issued upon the certification from the FBI that the information requested is "relevant to an international terrorism or espionage investigation."[122] Therefore, they must fit within an exception to the Fourth Amendment warrant requirement if they are to fit within the domestic criminal regulatory regime. As a comparison, administrative subpoenas are "at best, constructive searches," and as such they need not be supported by probable cause and need only be "reasonable."[123] But there are significant procedural differences between administrative subpoenas and NSLs, most importantly differences in judicial review, which may result in administrative subpoenas being reasonable while NSLs are not.[124]

The next sections will examine the "special-needs" exception and a more general, totality of the circumstances reasonableness test.

A. Special-Needs Exception and NSLs

NSLs, aside from being issued without judicial review, are issued without a showing that the target of the search is a terrorist or a terrorist supporter—the FBI merely "certifies" that the information requested is relevant to a counter-terrorism investigation.[125] While ordinarily a search must be based on an individualized suspicion of wrongdoing, when the risk to the public safety is substantial and real, a suspicionless search may still be "reasonable" and not violate the Fourth Amendment, even if one of the

120. *Cf. In re* Grand Jury Proceedings, 486 F.2d 85, 92 (3d Cir. 1973) (holding grand jury subpoena to not be a "search").

121. Op-Ed., Rachel Brand & John Pistole, Fed. Bureau of Investigation, *The Use and Purpose of National Security Letters*, *available at* http://www.fbi.gov/page2/natsecurityletters.htm (last visited Sept. 26, 2006) [hereinafter FBI Use and Purpose Memo].

122. *Id.*

123. *See* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946); *see also* United States v. Morton Salt Co., 338 U.S. 632, 651-52 (1950).

124. *Cf.* United States v. Bailey, 228 F.3d 341, 348 (4th Cir. 2000).

125. 18 U.S.C. § 2709 (2006).

goals is criminal prosecution.[126] The Supreme Court has long held that "the Fourth Amendment imposes no irreducible requirement of [individualized] suspicion"[127] and "in certain limited circumstances, the Government's need . . . is sufficiently compelling to justify the intrusion on privacy entailed by conducting such searches without any measure of individualized suspicion."[128] Accordingly, an NSL unsupported by individualized suspicion may be consistent with the Fourth Amendment if it fits within the confines of the special-needs doctrine.

The doctrine of special needs addresses situations where circumstances beyond an ordinary need for law enforcement make the warrant/probable cause requirement of the Fourth Amendment impracticable.[129] The special-needs exception seems especially applicable in an analysis of NSLs because they too blur the line between law enforcement and another legitimate governmental purpose—national security.

To apply the exception, the court first determines if a special need exists, and then determines whether the state's interest in that special need outweighs the privacy interest of the individual searched.[130] Some examples of circumstances where a special-needs exception was applied include the search of probationers' homes when probation officers have "reasonable grounds" to believe that contraband is present,[131] as well as the drug testing of high school athletes,[132] DEA employees in sensitive positions,[133] and locomotive engineers involved in a railway accident.[134] Two recent Supreme Court cases, however, demonstrate that warrantless searches will fall outside the special-needs exception to the Fourth Amendment when they serve the primary purpose of general crime

126. Chandler v. Miller, 520 U.S. 305, 305-06 (1997).

127. Bd. of Educ. of Ind. Sch. Dist. No. 92 of Pottawatomie Co. v. Earls, 536 U.S. 822, 829 (2002) (citing United States v. Martinez-Fuerte, 428 U.S. 543, 561 (1976)).

128. *Id.* (citing Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 668 (1989)); *see also* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602 (1989).

129. *See* Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (quoting New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring)).

130. *Id.* at 873-76.

131. *Id.* at 870-71.

132. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 665 (1995) (permitting drug testing of high school student athletes to protect their health).

133. *See* Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 667 (1989) (upholding mandatory drug testing for DEA agents employed in specific sensitive positions).

134. *See* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 633 (1989) (permitting mandatory drug testing of locomotive engineers following a railway accident). *But see* Chandler v. Miller, 520 U.S. 305, 322 (1997) (finding that purported special need for drug testing candidates for public office in Georgia did not fall into category of permissible suspicionless searches, in light of the candidates' privacy interests).

control.[135] In *Indianapolis v. Edmond*, the Court invalidated a highway checkpoint program on the grounds that the primary purpose was general crime control, despite the secondary purposes of driver safety and disaster prevention.[136] The following year, in *Ferguson v. Charleston*, the Court further held that a government program with the primary purpose of crime control did not outweigh the privacy interests of pregnant mothers unless the drug testing was done with their consent.[137]

The most recent Supreme Court case to address the question of special needs, *Illinois v. Lidster*, expanded the scope of permissible warrantless searches by allowing them where the primary purpose of the law is "information-seeking."[138] The Court recognized that despite the holding in *Edmond*, there are instances in which a purpose other than the need for law enforcement can relate to law enforcement activity, yet still justify a search without individualized suspicion.[139]

For NSLs to fulfill the requirements of the special-needs exception, they would have to serve a primary purpose other than the need for ordinary law enforcement. Evidence of a special purpose may be found in the ECPA itself; the ECPA includes a provision allowing law enforcement to obtain electronic records in domestic criminal investigations.[140] Therefore, because NSLs address access to the same records as section 2703, but for a different purpose, it seems that they serve a purpose outside of ordinary law enforcement.

Regardless of whether or not NSLs have a primary purpose beyond the need for ordinary law enforcement, they are reasonable under the totality of the circumstances. Notwithstanding the special-needs exception, warrantless searches can still be reasonable under the Fourth Amendment. The Court has held that special-needs cases are actually "limited exception[s]" to the traditional Fourth Amendment totality of the circumstances reasonableness analysis.[141] Further, "there is no basis for examining official purpose" under the totality of the circumstances test, as

135. *See* Ferguson v. City of Charleston, 532 U.S. 67, 81 (2001) (holding that drug testing of obstetrics patients for the purpose of crime control was unreasonable); Indianapolis v. Edmond, 531 U.S. 32, 48 (2000) (holding highway checkpoints for the purpose of drug interdiction do not serve a special need).

136. *Edmond*, 531 U.S. at 43, 47-48.

137. *Ferguson*, 532 U.S. at 85-86.

138. 540 U.S. 419, 424 (2004).

139. *Id.*

140. *See* 18 U.S.C. § 2703 (2006) (allowing a government entity to require an electronic service provider to turn over stored electronic records if the government obtains a warrant from a criminal court).

141. United States v. Knights, 534 U.S. 112, 122 (2001).

would be required by the special needs test.[142] Even if the primary purpose of the search is general law enforcement, the warrantless search is still permissible under the totality of the circumstances so long as the government's legitimate interests outweigh the privacy interest of the individual.[143]

Totality of the Circumstances

To analyze NSLs under a general reasonableness balancing test, it would certainly be helpful to have access to information regarding the use and effectiveness of NSLs in counter-terrorism operations. Michael J. Woods, former chief of the FBI's National Security Law Unit, makes the argument that the types of transactional records that can be gathered using NSLs are an "extraordinarily valuable source of data for counterintelligence analysts" because it is far more difficult for terrorists to cover up their "transactional footsteps" than it is for them to cover the substance of their communications.[144] Furthermore, it has been argued that NSLs help expedite the process of following up on terrorist threats and tips in a timely manner.[145] Judge Victor Marrero of the Southern District of New York, despite opposing unchecked NSL power, nonetheless agrees that efficiency in national security investigations is valuable.[146] National security is clearly "a paramount value, unquestionably one of the highest purposes for which any sovereign government is ordained."[147]

On the other side of the balancing test, one must consider the individual's privacy interests. As explored earlier in the discussion of the third party doctrine,[148] there is arguably a diminished privacy interest in information voluntarily turned over to a third party.[149] If the risk of abuse of NSL power is great enough, however, it can potentially shift the balance towards finding NSLs unreasonable under a totality of the circumstances balancing test.

142. *Id.* (upholding a warrantless search of a probationer's apartment because the government's reasonable suspicion of wrongdoing outweighed a probationer's diminished expectation of privacy).

143. *Id.* at 119.

144. Woods, *supra* note 6, at 41-42.

145. FBI Use and Purpose Memo, *supra* note 121.

146. Doe v. Ashcroft, 334 F. Supp. 2d 471, 476 (S.D.N.Y. 2004) ("To perform its national security functions properly, government must be empowered to respond promptly and effectively to public exigencies as they arise . . . .").

147. *Id.*

148. *See supra* notes 61-63 and accompanying text.

149. *See* United States v. Miller, 425 U.S. 435, 440-43 (1976).

1. Potential for Abuse

Several factors may increase the potential for abuse of NSLs. These are: (1) their secretive nature;[150] (2) the lack of oversight;[151] and (3) the fact that important decisions are placed in the hands of low-level officers.[152] Arguably, the most compelling factor indicating a potential for abuse of NSL power is the blurring of the line between foreign intelligence investigations and ordinary domestic criminal investigations.

The Framers of the Constitution relied upon separation of powers and a system of checks and balances to protect individual citizens from potential abuse of civil liberties.[153] There is a long history of such abuse in the realm of domestic intelligence investigations.[154] For example, the FBI, CIA, Army, and other agencies have carried out investigations that far exceeded their intended scope.[155] Perhaps the most famous example is the FBI's domestic counter-intelligence program ("COINTELPRO"), which was "designed to 'disrupt' groups and 'neutralize' individuals deemed threats to national security."[156] Under COINTELPRO, the government targeted political opponents in order to discredit them in the eyes of the public,[157] used the IRS to initiate tax investigations against political opponents,[158] targeted "speakers, teachers, writers, and publications" in

150. The First Amendment impact of secrecy is outside the scope of this Note.

151. *See infra* notes 173-78 and accompanying text.

152. *See* Krent, *supra* note 47, at 95. Generally, the changes to NSLs under the PATRIOT Act do exactly what Framer James Otis warned of—they place too much power and discretion in the hands of low-level law enforcement officers. Otis argued that low-level officers were more likely to abuse their power either due to a lack of judgment or for personal motivations. *Id.*

153. *Id.* at 94 (citing THE FEDERALIST NO. 62, at 333 (James Madison) (J.R. Pole ed., 2005) (having two separate houses of Congress "doubles the security to the people by requiring the concurrence of two distinct bodies in schemes of usurpation or perfidy"); THE FEDERALIST NO. 73, at 392 (Alexander Hamilton) (J.R. Pole ed., 2005) (stating that the requirement that the President approve new laws provides "an additional security against the enaction of improper laws")).

154. *See* Swire, *supra* note 78, at 1316; see also SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, 94TH CONG., FINAL REPORT ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, Book II, § I (1976) [hereinafter CHURCH REPORT IIA], *available at* http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIa.htm.

155. CHURCH REPORT IIA, *supra* note 154 , § 1 ("The tendency of intelligence activities to expand beyond their initial scope is a theme which runs through every aspect of our investigative findings. Intelligence collection programs naturally generate ever-increasing demands for new data.").

156. *Id.*

157. *Id.*

158. MARTIN HALPERIN ET AL., THE LAWLESS STATE: CRIMES OF THE U.S. INTELLIGENCE AGENCIES 191-94 (1976).

attempt to chill political opponents' First Amendment speech rights,[159] and generally infringed the "values of privacy and freedom which our Constitution seeks to protect."[160]

With NSLs, the potential for abuse also arises from the fact that the information obtained under foreign intelligence standards can be misused. If an investigation simply has as a "significant purpose" the gathering of intelligence on a suspected terrorist or terrorist supporter, what safeguards are in place to stop the investigators from turning over all of the information to a criminal prosecutor? Moreover, what would prevent a prosecutor or, perhaps, an individual in the administration with a political motivation, from suggesting to a Special Agent in Charge of a field office that he should certify that a particular person is being targeted as part of an "authorized investigation" and use an NSL to obtain Internet or telephone records for that individual? The potential for abuse of NSLs is certainly great, but the answer to the question of "reasonableness balancing" may turn on one's view of which is more important: civil liberties or national security. As more information about actual abuse of NSL power becomes public, however, perhaps the balance will shift towards stricter protections for privacy.[161]

PART III. HOW TO DELIVER A SAFER NSL

The previous section left open the question of whether NSLs could fit within an exception to the Fourth Amendment's warrant requirement. It does seem there are a sufficient number of arguments for fitting NSLs within a domestic regulatory scheme, if necessary, including: (1) NSLs are not "searches" and therefore need not satisfy the Fourth Amendment probable cause standard; (2) NSLs are foreign intelligence tools and accordingly do not require warrants unless they go beyond the standards set forth in 50 U.S.C. § 1802(a)(1); (3) NSLs have a purpose beyond ordinary law enforcement and therefore satisfy the special-needs exception; or (4) NSLs are reasonable under the totality of the circumstances. Regardless of how one classifies NSLs, there are steps that can be taken to safeguard civil liberties, while allowing the FBI to retain the power to issue NSLs. There are several potential avenues for oversight of NSLs including intra-agency regulations, ex ante judicial monitoring, ex post judicial review, legislative oversight, and public advocacy.

159. CHURCH REPORT IIA, *supra* note 154, § 1.

160. *Id.*

161. *But cf.* David Kirkpatrick & Scott Shane, *G.O.P. Senators Say Accord is Set on Wiretapping*, N.Y. TIMES, Mar. 8, 2006, at A1.

A. Administrative Checks

One possible defense against abuse is the internal check on surveillance powers from within the law enforcement agency.[162] First, the FBI Office of General Counsel issued a memo advising agents how to use NSLs correctly.[163] This memo suggests that NSLs should be used "judiciously" because they are "powerful investigative tools."[164] Furthermore, the memo advises field offices to "establish[] and enforce[] an appropriate review and approval process for the use of NSL authorities."[165]

In addition, each law enforcement and intelligence agency has an internal review board to investigate impropriety within the agency.[166] Those internal review boards may provide a safeguard against abuse, because they work in the same agency as the investigators and would have the easiest access to the entire record without allowing classified information from leaving the office. But is it wise to entrust the policing of investigations to the very same agencies that carry them out? For instance, it is unknown whether internal oversight officers are given sufficient resources or have sufficient motivation to effectively monitor the investigators.[167] While the agencies may be equipped to provide a first line of defense against abuse, perhaps oversight is better left to external "watchdogs."[168] Internal monitoring can also be problematic when the agency both defines the meanings of the terminology in the applicable statutes and then enforces the laws according to their own interpretations. For example, while the FBI Office of General Counsel's memo on NSLs explains that they may be issued "during the course of a full international terrorism or foreign counterterrorism investigation," but "cannot be used in criminal investigations unrelated to international terrorism or clandestine intelligence activities," it allows for NSLs to be issued in preliminary investigations where the nexus to counterterrorism has not yet been established.[169] If an investigation is authorized under FCIG its purpose is

162. Seth Kreimer, *Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror*, 7 U. PA. J. CONST. L. 133, 178 (2004).

163. *See generally* FBI NSL Memo, *supra* note 22.

164. *Id.* at 3.

165. *Id.*

166. Kreimer, *supra* note 162, at 178; s*ee also* Eric Lichtblau, *Justice Department Investigators Find a Cover-Up in an F.B.I. Terror Case in Florida*, N.Y. TIMES, Dec. 4, 2005, at 37.

167. Kreimer, *supra* note 162, at 178.

168. *Id.*

169. FBI NSL Memo, *supra* note 22, at 2-3. To issue an NSL for a preliminary investigation, the investigation must be authorized by the Attorney General's Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations

presumptively to "protect against international terrorism or clandestine activities."[170] It is troubling that the very agency that is supposed to be limited by the "related to a foreign intelligence investigation" requirement is also charged with determining which investigations fall into that category. Additionally, the fact that preliminary investigations are permitted to fall into this category means that practically any investigation, at least at the initial stage, may allegedly be connected to foreign intelligence and thus, allow access to almost any records that law enforcement wants to examine.

B. Judicial Oversight

Judicial oversight can be divided into two categories: ex ante judicial monitoring and ex post judicial review.[171] As previously established, judicial approval is not required to issue an NSL.[172] One obvious way to address the Fourth Amendment concerns regarding the reasonableness of NSLs would be to require prior judicial approval. NSLs could be subject to a standard similar to that used to obtain Title III wiretaps.[173] Some would surely argue that this requirement would be overly burdensome on both investigators and judicial resources. Nevertheless, judicial approval has been required in many types of domestic investigations and has not proven unduly burdensome. Alternatively, because NSLs are tools for foreign intelligence, they can be placed under the auspices of FISA and be subject to approval from the FISC before an NSL can be issued. This would ensure that sensitive information relating to terrorism investigations would be handled carefully and cautiously. The FISC can also ensure expedited processing that an ordinary court may not be able to provide.[174] Furthermore, the long term and ongoing nature of a terrorism investigation makes it difficult to present specific facts to a judge to show probable cause; placing NSLs under the jurisdiction of the FISA court would both

("FCIG"). *Id.*

170. *Id.*

171. Ex ante judicial oversight derives from a statutory requirement of court approval, such as a typical domestic criminal search warrant. *See* LA FAVE, SEARCH AND SEIZURE, *supra* note 42, at § 4.1. Ex post judicial oversight refers to the eventual contestability of suspect searches or the fruits thereof by the parties searched. *See id.*

172. *See supra* note 26 and accompanying text.

173. *See* Title III of the Omnibus Crime and Control and Safe Streets Act of 1968, 18 U.S.C. § 2511 (2002).

174. The FISC has eleven judges who specialize in national security matters. 50 U.S.C. § 1803(a) (2006). They work around the clock to process FISA requests. Additionally, the FISC has a seventy-two-hour delay provision to allow emergency orders to be reviewed within seventy-two hours without requiring law enforcement to wait for the FISC to convene. 50 U.S.C. § 1801(h)(4).

maintain the government's ability to get NSLs authorized where needed, while providing an extra check on unfettered executive branch power.

Ex post judicial review is another option to help safeguard privacy interests while still allowing the FBI to use NSLs for national security purposes. NSLs could be redrafted to specifically inform their recipients of their right to go to court to challenge the reasonableness of the NSL. Part of the government's justification for the constitutionality of NSLs is that they are not searches, but merely information requests. As a practical matter, however, very few recipients would feel such a request is "voluntary" when the FBI shows up with an NSL, asks the recipient to bring the requested records to the FBI's office, and states that the recipient cannot tell *anyone* about the NSL. Explicitly stating that NSLs are not court-ordered could eliminate concerns that NSLs are compulsory searches and as such must be approved by a court in order to be constitutional. Another option is to have ex post judicial monitoring structured in a manner comparable to the monitoring required for a Title III order.[175] This may in fact be less burdensome than Title III because investigators will not need prior approval and will follow a monitoring procedure that they are quite familiar with in the domestic criminal realm.

C. Legislative Oversight

Generally, when members of the public are concerned about a law, the official "answer" is that they should contact their congressman. With regard to NSLs, the DOJ has asserted that Congress is actively involved in monitoring their use, and that the public should be assured that their elected representatives are looking out for their privacy interests.[176] This reasoning fails to take into account several key points. First, in a representative democracy, elected officials are heavily influenced by public opinion. It is hard to rely on Congress to protect our privacy rights if members of the public are unaware that NSLs are being issued and therefore are not actively involved in seeking congressional intervention on their behalf. Second, the DOJ explanation ignores the partisan politics prevalent in the congressional oversight process. For example, the chair of the Judiciary or the Intelligence committees in either house of Congress

175. Title III wiretaps require reporting to the magistrate who authorized them. *See* 18 U.S.C. §§ 2518-19. Not only does Title III require prior judicial approval, it includes procedures to safeguard the rights of the individuals whose communications are intercepted. *See* 18 U.S.C. §§ 2510-22.

176. *See generally* U.S. Dep't of Justice, Questions About the USA PATRIOT Act, http://www.lifeandliberty.gov (last visited Sept. 26, 2006).

could issue a Congressional subpoena to compel more complete disclosure from the FBI on the use of NSLs. Of course, "the minority has no power to compel, and . . . Republicans are not going to push for oversight of the Republicans."[177]

Effective legislative oversight requires both the cooperation of the DOJ, with regard to accurate reporting of the use of NSLs, as well as the ability of recipients to inform their representative that an NSL was issued. Congressional oversight, while potentially valuable, is too dependent on information obtained from the DOJ for its effectiveness.[178] Those who support the continued use of NSLs do not want to doubt the accuracy of the DOJ's numbers, but self-reported numbers may have a greater potential for misrepresentation without external verification. The gag order provision of section 2709(c) would prevent a constituent from disclosing the issuance of an NSL; without the efforts of external groups, possible governmental abuses of NSL power may not be brought to the public's attention.

D. Non-governmental Advocacy Groups

While it is possible for the legislature and the courts to provide checks on executive power and still maintain the secrecy of investigations,[179] perhaps the most effective oversight comes from non-governmental civil liberties groups, such as the American Civil Liberties Union ("ACLU") and the Electronic Privacy Information Center ("EPIC"). These groups can initiate lawsuits to obtain records and documents to track the use of NSLs.[180] In 2004, internal FBI reviews identified 113 violations of federal law or bureau policy—again, presumably involving the use of NSLs—most of which related to intelligence or national security investigations.[181] While "watchdog" groups are important sources of information for the public,[182] there is a tendency to exaggerate the threat that NSLs actually present. Such slanted presentation may result in public resentment and may ultimately undermine the valuable service that such groups provide.[183]

177. Gellman, *supra* note 1, at A1 (quoting Rep. Zoe Lofgren (D-Cal.), a House Judiciary Committee member).

178. *See* Dahlia Lithwick & Julia Turner, *A Guide To the PATRIOT Act, Part 1: Should You Be Scared of the PATRIOT Act?*, SLATE, Sept. 8, 2003, http://www.slate.com/id/2087984/ (describing how FOIA requests have been incomplete and Congressional requests have been ignored or classified).

179. Kreimer, *supra* note 162, at 178.

180. *Id.*

181. *See* Eric Lichtblau, *Tighter Oversight of F.B.I. Is Urged After Investigation Lapses*, N.Y. TIMES, Oct. 25, 2005, at A16.

182. FOIA requests have allowed public access to DOJ documents.

183. *See* Eric Lichtblau, *Ashcroft Mocks Librarians and Others Who Oppose Parts of*

IV. CONCLUSION

Notwithstanding concerns over the lack of safeguards and intrusions into privacy, NSLs have existed for nearly twenty years and are likely to continue to be used. Effective oversight is essential to making NSLs an acceptable tool for law enforcement. While the Department of Justice has not given specific information on how NSLs are used and whether or not they have proved to be useful, there is great value in giving law enforcement and intelligence agencies the tools they need to do their jobs to keep our country safe.[184] But as Benjamin Franklin observed over 200 years ago, "they that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."[185] The Framers of our Constitution were wary of the potential for abuse in giving the executive the power to search a man's home or seize his property without requiring the specification of the reason for the search and what the search was expected to uncover to a neutral party.[186] Furthermore, they believed that power in the hands of one branch of government, without meaningful and thorough oversight by the other branches, would lead to overreaching and infringement upon individual civil liberties.[187] Following 9/11, however, the political climate in the United States, perhaps understandably, became less protective of civil liberties and more interested in safeguarding our borders and our cities.[188] In fact, a recent poll suggests that this attitude continues five years later and that Americans have expressed a willingness to tolerate invasions of privacy without warrants in order to fight terrorism, despite being wary of the impact these types of actions might have on civil liberties.[189] Unfortunately, in light of recent revelations about the executive branch's use of illegal—or at the very least, questionably legal—wiretaps to spy on U.S. citizens,[190] the changes made to many existing laws under the PATRIOT Act may continue to take this country further away from the vigorous protections intended by the Constitution and the Bill of Rights.

Counterterrorism Law, N.Y. TIMES, Sept. 16, 2003, at A23.

184. *See generally* Doe v. United States, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

185. *See* JOHN BARTLETT, FAMILIAR QUOTATIONS 348 (Emily Morrison Beck ed., 1980).

186. U.S. CONST. amend IV.

187. Krent, *supra* note 47, at 94-95.

188. *Doe*, 334 F. Supp. 2d at 471.

189. Adam Nagourney & Janet Elder, *New Poll Finds Mixed Support for Wiretaps*, N.Y. TIMES, Jan. 27, 2006, at A1.

190. *See* Transcript, *U.S. Senate Judiciary Committee Holds a Hearing on Wartime Executive Power and the NSA's Surveillance Authority*, WASH. POST., Feb. 6, 2006 (online edition), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020600931.html.