

National Security Letters and the Amended Patriot Act

Andrew E. Nieland

Follow this and additional works at: <http://scholarship.law.cornell.edu/clr>

 Part of the [Law Commons](#)

Recommended Citation

Andrew E. Nieland, *National Security Letters and the Amended Patriot Act*, 92 Cornell L. Rev. 1201 (2007)
Available at: <http://scholarship.law.cornell.edu/clr/vol92/iss6/4>

This Note is brought to you for free and open access by the Journals at Scholarship@Cornell Law: A Digital Repository. It has been accepted for inclusion in Cornell Law Review by an authorized administrator of Scholarship@Cornell Law: A Digital Repository. For more information, please contact jmp8@cornell.edu.

NOTE

NATIONAL SECURITY LETTERS AND THE AMENDED PATRIOT ACT

Andrew E. Nieland†

INTRODUCTION	1201
I. A BRIEF HISTORY OF THE NATIONAL SECURITY LETTER	1206
A. The Origins of NSL Authority	1207
B. NSL Authority and the 2001 Patriot Act	1211
C. The Covert Expansion of 18 U.S.C. § 2709.....	1213
II. THE NSL CASES AND THE AMENDED PATRIOT ACT	1215
A. <i>Doe v. Ashcroft</i>	1215
B. <i>Doe v. Gonzales</i>	1220
C. Congressional Response to the NSL Cases	1224
III. A CRITIQUE OF THE AMENDED PATRIOT ACT.....	1226
A. The Shortcomings of the NSL Debate	1226
B. The Amended NSL Statutes and Civil Liberties	1227
C. How the Amended Patriot Act Hampers NSL Efficacy.....	1231
1. “Self-Help” as an Alternative to Contempt.....	1231
2. <i>How Much Judicial Review Is Enough?</i>	1233
a. <i>Must an NSL Recipient Be Allowed to Initiate Judicial Review?</i>	1233
b. <i>When and How Must Nondisclosure Be Reviewed?</i>	1235
CONCLUSION: HARMONIZATION OR DISCORD?	1236

INTRODUCTION

For nearly two decades, various statutes have authorized the Federal Bureau of Investigation to issue “national security letters” (NSLs)—formal demands to surrender certain records and refrain from disclosing the fact of the request. Like other forms of compulsory process, such as the grand jury subpoena, the NSL makes a legal threat: “Hand over these records and keep quiet about it, or else.”

† A.B., Harvard College, 1997; J.D., Cornell Law School, 2007. I am grateful to Professors Steven Clymer and Trevor Morrison for their insights on this topic, and to my colleagues at the *Cornell Law Review*, especially Aaron Stewart, Arthur Andersen, Ken Meyer, and Kyle Taylor for their careful editing.

Remarkably, over fifteen years and hundreds of NSLs, not one recipient had the temerity to ask “Or else *what?*”

Thus, until very recently, the NSL statutes provided a rare example of an unbroken law. Recipients of such letters apparently never challenged their validity, and the FBI never had to seek a contempt order to assure compliance.¹ The letters likely owe much of their success to the stringent secrecy requirements surrounding them: Under the authorizing statutes, the first of which was passed in 1978,² recipients cannot disclose to “any person” the fact that they have received an NSL.³ Under a reasonable interpretation of this language, a recipient could break the law by telling his employer—or even his lawyer—about the letter.⁴

Over the years, the FBI has repeatedly sought to expand the circumstances under which its agents could issue NSLs.⁵ Congress delivered a particularly robust expansion in section 505 of the USA PATRIOT Act of 2001 (Patriot Act),⁶ which allowed the FBI to issue an NSL in circumstances roughly comparable to those in which a federal prosecutor could obtain a grand jury subpoena.⁷ After the Patriot Act’s passage, the number of NSLs issued apparently⁸ exploded—

¹ See *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 502 (S.D.N.Y. 2004), *vacated and remanded sub nom. Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006).

² The Right to Financial Privacy Act (RFPA) authorized various agencies to request financial records under a form of NSL authority. See *infra* Part I. Although requests were not mandatory, RFPA forbade the recipient from disclosing that he had either received or complied with such a request. See *id.*

³ See, e.g., 18 U.S.C. § 2709(c) (2000).

⁴ See *Ashcroft*, 334 F. Supp. 2d at 475.

⁵ See *infra* Part I.

⁶ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S.C.).

⁷ See *Ashcroft*, 334 F. Supp. 2d at 482–84 (noting that the drafters replaced the “nexus to a foreign power” requirement and replaced it with a “broad standard of relevance to investigations of terrorism or clandestine intelligence activities,” in an attempt to “harmonize[]” section 2709 with a federal prosecutor’s power to issue a grand jury subpoena (citation omitted)).

⁸ The Justice Department released a “partial” classified tally of NSL usage to Congress but made no public reporting of NSL statistics prior to 2006. See Barton Gellman, *The FBI’s Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, WASH. POST, Nov. 6, 2005, at A1.

from “hundreds” between 1978 to 2001,⁹ to perhaps “more than 30,000” per year from 2002 to 2005.¹⁰

Despite this sea change in FBI procedure, NSLs received little public attention until 2004, when an anonymous Internet Services Provider (ISP) received an NSL and challenged its validity in federal court.¹¹ In *Doe v. Ashcroft*, the district court awarded summary judgment for this plaintiff, holding that one of the NSL statutes, as applied, violated the Fourth Amendment by effectively barring any judicial challenge to the compulsory demand for information, and violated the First Amendment as a content-based prior restraint on speech.¹²

In August 2005, a second NSL recipient challenged the same statute in the District of Connecticut.¹³ Two unique features of this case, *Doe v. Gonzales*, brought NSLs to the forefront of the national debate over the Patriot Act. First, the *Gonzales* plaintiffs wanted to announce the fact that they had received an NSL, and did not wish to wait for a victory on the merits to do so.¹⁴ Speed was critical, the plaintiffs argued, since Congress was currently debating various amendments to and extensions of the Patriot Act, and their experiences—valuable evi-

⁹ See *Ashcroft*, 334 F. Supp. 2d at 502 (basing this estimate on the “long time span” between the passage of the first NSL statute and the present day, and information obtained via the Freedom of Information Act showing that “hundreds” of NSLs had been requested between 2001 and 2003). The FBI’s Inspector General has subsequently asserted a much higher yearly tally—8500 requests in 2000, and 7800 in 1999. OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF NATIONAL SECURITY LETTERS 44 n.84 (2007), <http://www.usdoj.gov/oig/special/s0703b/final.pdf>. [hereinafter NSL AUDIT].

¹⁰ The oft-repeated 30,000-per-year figure was first reported in November 2005 by *Washington Post* reporter Barton Gellman. See Gellman, *supra* note 8. The day after Gellman’s article ran, the *New York Times* reported that “F.B.I. officials declined . . . to say how many letters the bureau had issued but expressed some skepticism about the accuracy of the 30,000 figure.” Eric Lichtblau, *Lawmakers Call for Limits on F.B.I. Power to Demand Records in Terrorism Investigation*, N.Y. TIMES, Nov. 7, 2005, at A20. Gellman insists that his figure is accurate and retorted that the “skeptical” lack of an express denial was a tactic used by unnamed sources to deal with “a fact they don’t want to, or can’t, deny.” Barton Gellman, *Washingtonpost.com*, The FBI’s Secret Scrutiny (Nov. 7, 2005), <http://www.washingtonpost.com/wp-dyn/content/discussion/2005/11/07/DI2005110700495.html>. The Inspector General has subsequently estimated that the FBI issued over 39,000 requests annually between 2003 and 2005. See NSL AUDIT, *supra* note 9, at 37 chart 4.1. But because each physical letter may request information on numerous phone numbers or individuals, the number of letters issued during this period is smaller. See *id.* at 4 & chart 1.1.

¹¹ See *Ashcroft*, 334 F. Supp. 2d at 475.

¹² See *id.*

¹³ See *Doe v. Gonzales*, 386 F. Supp. 2d 66, 69 (D. Conn. 2005), *dismissed as moot*, 449 F.3d 415, 420 (2d Cir. 2006).

¹⁴ See *id.* at 70. Elsewhere, the judge notes that the Government “agreed to the docketing of the Redacted Complaint, which reveals that an investigation (of unknown topic) exists and that a[n] NSL was issued in Connecticut to an organization with library records.” *Id.* at 81.

dence of the way the law actually worked—were “relevant and perhaps crucial to an ongoing and time-sensitive national policy debate.”¹⁵ As a result, they sought a preliminary injunction against the enforcement of the statute’s secrecy provision.¹⁶

Second, the NSL recipient in *Gonzales* possessed “information about library patrons” because he was “a member of the American Library Association,” (ALA).¹⁷ Although it had little legal significance,¹⁸ this fact had tremendous rhetorical import. Library organizations like the ALA were among the most vocal critics of other provisions of the Patriot Act.¹⁹ In one notorious skirmish, former Attorney General John Ashcroft dismissed their main concern—that the FBI would use the Patriot Act to monitor America’s reading habits—as “hysteria.”²⁰ For opponents of the Patriot Act, the *Gonzales* case seemed to provide a rare “gotcha!” moment, concrete proof that the Bush administration was using the Act to trample civil liberties in a misguided crusade against terror.²¹

As the *Gonzales* litigation raced through the tiers of the federal judiciary, the NSLs’ public notoriety increased. In less than a month, the district court granted the plaintiffs’ injunction but ordered a brief stay to allow the Government to appeal;²² the Second Circuit extended the stay;²³ and Justice Ruth Bader Ginsburg, sitting as Circuit

¹⁵ *Id.* at 70.

¹⁶ *See id.*

¹⁷ *Id.*

¹⁸ The challenged statute applies to any “wire or electronic communication service provider,” but limits the information obtainable via NSL to “subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession.” 18 U.S.C. § 2709(a) (2000). This section of the Patriot Act did not initially receive much scrutiny from either civil rights groups or library organizations—for example, a report on the important changes made by the Patriot Act, prepared for the American Association of Law Libraries by the Washington, D.C., firm of Wiley Rein & Fielding, did not even mention section 505. *See* WILEY REIN & FIELDING LLP, THE SEARCH & SEIZURE OF ELECTRONIC INFORMATION: THE LAW BEFORE AND AFTER THE USA PATRIOT ACT (2001), <http://www.aallnet.org/aallwash/uspatriotbefaft.pdf> (the document is dated January 18, 2001, which must be incorrect because Congress had not yet drafted the Patriot Act, and was presumably issued in January of 2002).

¹⁹ *Cf.* John Ashcroft, Attorney Gen. of the U.S., Protecting Life and Liberty (Sept. 18, 2003), [available at http://www.usdoj.gov/archive/ag/speeches/2003/091803memphisremarks.htm](http://www.usdoj.gov/archive/ag/speeches/2003/091803memphisremarks.htm).

²⁰ *See id.* (“The fact is, with just 11,000 FBI agents and over a billion visitors to America’s libraries each year, the Department of Justice has neither the staffing, the time nor the inclination to monitor the reading habits of Americans. No offense to the American Library Association, but we just don’t care.”).

²¹ *See, e.g.*, Editorial, *Excessive Powers*, N.Y. TIMES, Aug. 27, 2005, at A12 (“[C]ivil libertarians opposed the provision not because they knew it had been used . . . but because they expected it would be. It turns out that they were right to be concerned.”).

²² *See Gonzales*, 386 F. Supp. 2d at 82–83 (ordering an eleven-day stay of judgment).

²³ *See* Alison Leigh Cowan, *Librarians Must Stay Silent in Patriot Act Suit, Court Says*, N.Y. TIMES, Sept. 21, 2005, at B2.

Justice, affirmed the extension,²⁴ even though a filing gaffe allowed the *New York Times* to discover and publish the plaintiff's identity—the secret the stay was designed to protect.²⁵ In November 2005, NSLs moved from the metro section to the front page when the *Washington Post* published a report claiming that the FBI had issued over 30,000 letters per year since the passage of the Patriot Act.²⁶ By December, the disagreement over the NSL statutes had become one of two main “sticking point[s]” that prevented Congress from passing an amended version of the Patriot Act before the end of 2005, when other provisions of that law would sunset.²⁷

Congress finally amended the Patriot Act on March 9, 2006.²⁸ This legislation explicitly permits NSL recipients to consult a lawyer and seek judicial review of the letter's validity, much as recipients may challenge a subpoena.²⁹ The amended Act also tailors the secrecy requirement—the FBI may still “gag” recipients indefinitely, but it must certify that a need for secrecy exists³⁰ and recertify annually if the recipient challenges that necessity.³¹ In so doing, this legislation closes the statutory lacunae that the *Gonzales* and *Ashcroft* courts found most troublesome.³² Unsurprisingly, both civil libertarians³³ and advocates of a more powerful FBI³⁴ rushed to portray the amendments as a victory.

This Note argues that in the battle over NSLs, everyone lost. The amendments do not signify Congress's heightened concern for citizens' privacy, its unwavering commitment to national security, or even a reasoned attempt to balance the two. The amendments merely indicate Congress's continued susceptibility to artful lobbying bolstered by

²⁴ See *Doe v. Gonzales*, 126 S. Ct. 1, 5 (2005), *ordered unsealed by and superseded by* 127 S. Ct. 1 (2005).

²⁵ See Cowan, *supra* note 23 (“Though the plaintiffs' organization has not been named in the various proceedings, a close reading of the court record suggests that it is Library Connection in Windsor, Conn. A search of a court-operated Web site offered a pointer to the plaintiffs' identity. There, a case numbered 3:2005cv01256 is listed under the caption, ‘Library Connection Inc. v. Attorney General.’”).

²⁶ See Gellman, *supra* note 8.

²⁷ See Elisabeth Bumiller, *Bush Renews Patriot Act Campaign*, N.Y. TIMES, Jan. 4, 2006, at A10. Lawmakers did agree to extend the provisions of the Act scheduled to expire at year's end until February 3, 2006. See *id.*

²⁸ USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, 120 Stat. 192 (codified as amended in scattered sections of the U.S.C.).

²⁹ See 18 U.S.C.A. § 3511 (Supp. 2006).

³⁰ See *id.* § 2709(c).

³¹ See *id.* § 3511.

³² See *infra* Part II.

³³ Critics of the Patriot Act were particularly pleased by the FBI's decision to drop the *Gonzales* appeal. See Anahad O'Connor, *Librarians Win as U.S. Relents on Secrecy Law*, N.Y. TIMES, Apr. 13, 2006, at B1; see also Editorial, *Civil Liberties Score Win vs. Patriot Act*, POST-STANDARD (Syracuse, N.Y.), Apr. 20, 2006, at A-10.

³⁴ See Editorial, *Renewing the Patriot Act*, CHI. TRIB., Mar. 13, 2006, at 20.

a high-profile case with a sympathetic plaintiff. In the heated debates over the judicial review and nondisclosure provisions, the partisans apparently forgot that they knew precious little about how this investigatory tool actually worked. As a result, national security advocates squandered an opportunity to fashion a more powerful tool, and civil libertarians forfeited a chance to craft a minimally intrusive one.

Part I discusses the evolution of the NSL statutes that culminated in the passage of the Patriot Act of 2001. It emphasizes two frequently overlooked facts about these statutes. First, it shows how NSLs began as an alternative to compulsory process—a way to “override” privacy legislation—but evolved into simply another form of compulsory process. Second, it emphasizes that the breadth of NSL authority expanded not merely overtly through legislative amendment, but also covertly through technological change. These facts help explain why NSL use exploded after Congress passed the Patriot Act. A careful scrutiny of this history also suggests why Congress failed to anticipate this explosion.

Part II discusses *Ashcroft* and *Gonzales*—the first legal challenges to the NSL statutes—and the 2006 amendments to those statutes. It emphasizes how the former strongly influenced, and likely overinfluenced, the latter. Part III critiques the amendments based on Parts I and II. It suggests that the lack of both a coherent oversight requirement and a sunset provision frustrates civil libertarian aims, and that the failure to imagine new forms of (or alternatives to) compulsory process stymies attempts to fight terrorism more effectively. In addition, Part III argues that the amendments give the FBI, through piecemeal amendment and technological happenstance, something that it had been unable to obtain through more overt political channels—a remarkably robust administrative subpoena power. Some may argue that this power goes too far, and others may insist that it does not go far enough. But both sides should be alarmed that the power has arisen so haphazardly and that Congress has not positioned itself to control it effectively.

I

A BRIEF HISTORY OF THE NATIONAL SECURITY LETTER

In the debate over the NSL statutes, confusion and misinformation abound. The editors of the *New York Times* have claimed, mistakenly, that the Patriot Act gave the FBI the power to obtain medical records via NSLs.³⁵ Partisans engage in semantic wrangling over

³⁵ See Editorial, *The Rush to Renew the Patriot Act*, N.Y. TIMES, Dec. 16, 2005, at A40 (“For example, the bill gives the government far too much power to issue ‘national security letters,’ demanding private financial, medical and library records, without the permission or oversight of a judge.”). This is incorrect. See *infra* note 38.

whether the *Ashcroft* decision actually struck down a provision of the Patriot Act as unconstitutional.³⁶ Even federal judges confuse section 505 of the Act, which concerns NSLs, with section 215, which concerns subpoenas issued by the Foreign Intelligence Surveillance Court (FISC).³⁷

Such confusion stems from myriad sources: the cloak of secrecy surrounding NSLs; the complexity of the Patriot Act and the extraordinary circumstances surrounding its passage; the nuanced distinctions between various types of compulsory process; the rhetoric of advocates of all stripes; and even investigative abuses of the NSL authority.³⁸ This Part seeks to dispel some of that confusion.

A. The Origins of NSL Authority

Ironically, the national security letter—that current *bête noire* of civil libertarians—originated in legislation designed to safeguard individual privacy. The first statute creating something resembling today’s NSL authority was the Right to Financial Privacy Act of 1978 (RFPA).³⁹ RFPA was a direct response to the Supreme Court’s controversial deci-

³⁶ See, e.g., *Oversight of the USA PATRIOT Act: Hearings Before the S. Comm. on the Judiciary*, 109th Cong. 385–86 (2005) (testimony of Bob Barr) (“A number of interested parties continue to claim, however, that *Doe v. Ashcroft* did not strike down a provision of the USA PATRIOT Act because section 2709, prior to the Act, did not contain a right to challenge and contained a gag order. This is inaccurate. First, whenever a statute is struck down in its entirety any then-operative amendments are also rendered unconstitutional. It is hard to see how a decision that strikes down every word of one section of a law can be said not to ‘involve’ that law. Second, analytically speaking, the USA PATRIOT Act is the 800-pound gorilla in the Marrero opinion, and clearly factored into his reasoning.”).

³⁷ In *Doe v. Gonzales*, 386 F. Supp. 2d 66, 74 n.6 (D. Conn. 2005), *dismissed as moot*, 449 F.3d 415 (2d Cir. 2006), the court asserts that the instant case, *Doe v. Ashcroft*, and a case in Detroit constitute the only challenges to national security letters. That statement appears to be inaccurate—the case in Detroit almost certainly refers to *Muslim Community Ass’n of Ann Arbor v. Ashcroft*, 459 F. Supp. 2d 592 (E.D. Mich. 2003), a 2003 challenge to section 215 of the Patriot Act, filed in the Eastern District Court of Michigan, which sits in Detroit. See, e.g., Fernando A. Bohorquez, Jr., *Challenges to Challenging the Patriot Act: Limits on Judicial Review and a Proposal for Reform*, N.Y. St. B.J., Feb. 2005, at 24, 27–28. Section 215 amended the Foreign Intelligence Surveillance Act of 1978 (FISA), which deals with subpoenas issued by the Foreign Intelligence Surveillance Court (FISC). See *id.* at 25. NSLs, on the other hand, are authorized by, *inter alia*, the Electronic Communications Privacy Act (ECPA) and merely require internal FBI certification rather than FISC approval. See *infra* Part I.A. *Ashcroft* and *Gonzales* challenge the ECPA amendments contained in section 505 of the Patriot Act, which relax the standards for issuing NSLs. See *infra* Parts II.A & II.B. Thus, these cases appear to be the only legal challenges to NSL authority ever raised.

³⁸ For example, the *New York Times’s* confusion about medical records, *supra* note 35, likely stems from an incident during the summer of 2005, when FBI agents attempted to use an NSL to obtain the medical records of a North Carolina State University student suspected in the London Underground bombings. See Gellman, *supra* note 8. A high-ranking FBI official described such usage as erroneous. See *id.*

³⁹ RFPA was, in turn, only Title XI of a massive banking regulation bill, the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641 (codified as amended throughout 12 U.S.C.).

sion in *United States v. Miller*,⁴⁰ which, according to Congress, stood for the proposition that "a customer of a financial institution has no standing under the Constitution to contest Government access to financial records."⁴¹ Generally, the Act provided that "when the Government seeks the records of a customer of a financial institution which are relevant to a legitimate law enforcement inquiry, it must employ a subpoena or formal written request reviewable in court, or obtain a search warrant," thereby giving the customer notice of the request and an opportunity to challenge it in court.⁴²

But the Act also provides a limited exception to these provisions "in the case of foreign intelligence, Secret Service protective functions and emergency situations."⁴³ In these circumstances, government agents could *request* financial records if a designated supervisor certified their requests.⁴⁴ Such disclosures, while exempt from the privacy safeguards of RFPA, were not mandatory.⁴⁵ However, the section did forbid the recipient from disclosing the fact of the request itself, although the statute did not provide a penalty for violating this bar.⁴⁶ The drafters intended that requests under this section would be used sparingly, and explicitly warned that "investigations proceeding only under the rubric of 'national security' do not qualify" for the exception.⁴⁷

Oddly enough, by 1986 the FBI was referring to such requests as "national security letter[s]."⁴⁸ It used the same term to refer to investigators' written requests for certain telephone records.⁴⁹ Recipients almost always complied with these voluntary requests, due in large part to a private agreement between the Justice Department and AT&T⁵⁰—far and away the largest telephone service provider at the

⁴⁰ 425 U.S. 435 (1976).

⁴¹ H.R. REP. NO. 95-1383, at 34 (1978), as reprinted in 1978 U.S.C.C.A.N. 9273, 9306.

⁴² S. REP. NO. 99-307, at 15 (1986) (discussing the 1978 Act and the 1986 amendments to its NSL authority provisions); see also 12 U.S.C. §§ 3401-3413 (2000).

⁴³ H.R. REP. NO. 95-1383, at 55.

⁴⁴ See 12 U.S.C. § 3414(a)(2).

⁴⁵ See *id.* § 3414(a)(1) ("Nothing in this chapter . . . shall apply to the production and disclosure of financial records pursuant to requests from [certain government authorities]."). Note that § 3414(a)(5), *requiring* financial institutions to comply, was not added until 1986. See Intelligence Authorization Act for Fiscal Year 1987, Pub. L. No. 99-569, § 404, 100 Stat. 3190, 3197 (1986) (codified as amended at 12 U.S.C. § 3414(a)(5)).

⁴⁶ See 12 U.S.C. § 3414(a)(3) ("No financial institution, or officer, employee, or agent of such institution shall disclose to any person that a Government authority described in paragraph (1) has sought or obtained access to a customer's financial records.").

⁴⁷ H.R. REP. NO. 95-1383, at 55.

⁴⁸ S. REP. NO. 99-307, at 15 (1986).

⁴⁹ See *id.* at 18-19 (discussing FBI requests for "telephone subscriber information or toll billing record information").

⁵⁰ See *id.* at 19.

time.⁵¹ However, as communications common carriers proliferated⁵² and many states enacted privacy laws prohibiting such voluntary disclosures, these NSLs met increasing resistance.⁵³ The FBI sought congressional intercession, which Congress granted to a limited extent in section 201 of the Electronic Communications Privacy Act of 1986 (ECPA).⁵⁴ Subsequent statutes also created a form of NSL authority with regard to credit records⁵⁵ and the records of certain government employees.⁵⁶ But both *Ashcroft* and *Gonzales* concern 18 U.S.C. § 2709, the codification of ECPA's NSL provisions.⁵⁷ That provision and its subsequent amendments are therefore the focus of this Note.

Like RFPA, from which it directly descends, ECPA was designed to be broadly protective of individual privacy.⁵⁸ To balance competing private and governmental interests, ECPA forbade government agencies from obtaining "stored electronic communications information" without the customer's permission, unless it did so "through compulsory process, such as a subpoena, warrant, or court order."⁵⁹

The only exception to this broad subpoena requirement was a newly mandatory form of NSL,⁶⁰ whose reach the statute constrained in four important respects. First, government agencies could, and still can, only issue requests to "wire or electronic communication services provider[s]."⁶¹ Second, ECPA limited the type of information thus obtainable to "subscriber information and toll billing records information."⁶² The Senate Intelligence Committee contemplated allowing access only to "telephone subscriber information or toll billing record information" since the federal courts did not require a warrant or probable cause to obtain such information.⁶³ The Judiciary Committee also added a provision allowing access to electronic communica-

⁵¹ See Wikipedia.org, American Telephone & Telegraph Company, http://en.wikipedia.org/wiki/AT%26T_%281885-2005%29 (last visited Aug. 12, 2007).

⁵² See *id.*

⁵³ See S. REP. NO. 99-307, at 19.

⁵⁴ See *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 480–81 (S.D.N.Y. 2004), *vacated and remanded sub nom. Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006). In the same year, Congress also added language making the RFPA NSLs mandatory. See 12 U.S.C. § 3414(a)(5)(A) (2000) ("Financial institutions . . . shall comply with a request . . . made pursuant to this subsection by the Federal Bureau of Investigation . . .").

⁵⁵ See 15 U.S.C.A. §§ 1681u–1681v (1998 & Supp. 2006).

⁵⁶ See 50 U.S.C. § 436 (2000).

⁵⁷ See *Doe v. Gonzales*, 386 F. Supp. 2d 66, 69 (D. Conn. 2005), *dismissed as moot*, 449 F.3d 415 (2d Cir. 2006); *Ashcroft*, 334 F. Supp. 2d at 475.

⁵⁸ See *Ashcroft*, 334 F. Supp. 2d at 480.

⁵⁹ *Id.* at 481 (citing 18 U.S.C. § 2703 (2000)).

⁶⁰ See 18 U.S.C. § 2709(a).

⁶¹ *Id.*

⁶² *Id.*

⁶³ S. REP. NO. 99-307, at 20 (1986) (citing Reporters Comm. for Freedom of the Press v. Am. Tel. & Tel. Co., 593 F.2d 1030 (D.C. Cir. 1978)).

tion transactional information, although it did not provide a clear rationale for doing so.⁶⁴

Third, the Act limited the types of investigations in which the FBI could use NSLs. The FBI had to certify both that 1) the information was "relevant to an authorized foreign counterintelligence investigation," and 2) there were "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."⁶⁵ Finally, ECPA limited who could provide such certification: only the Director of the FBI, "or an individual within the Federal Bureau of Investigation designated for this purpose by the Director."⁶⁶ Although the statute did not explicitly say so, its drafters did not intend for the director to delegate this authority lightly. The Senate Judiciary Committee reported that "[i]t is intended that the application of the 'reason to believe' requirement will be determined by a senior FBI official at the level of Deputy Assistant Director or above."⁶⁷

It thus bears repeating that NSL authority was initially intended as a limited alternative to, and not a form of, the compulsory process of a subpoena. The legislative history demonstrates that the drafters knew the RFPA provision "d[id] not provide for notice and an opportunity to litigate" and that they did not discuss including such a provision in either ECPA or the revised RFPA.⁶⁸ Also, the drafters did not include any mechanism for enforcing compliance with either the demand or the secrecy provision, and nothing in the record explains this omission. Under a fair reading of the 1986 statute, any other privacy legislation would not prevent NSL recipients from complying, but the statute could not force recipients to comply if they were otherwise unwilling to do so.⁶⁹ The statute forbade recipients from disclosing the fact of the demand, but did not specify the consequences of violating this provision.⁷⁰ The 1986 statute therefore made NSL authority less powerful than a subpoena, but perfectly sufficient in situations where state privacy legislation presented the only barrier to compliance.⁷¹

In 1993, Congress first relaxed the requirement of a "nexus" to a foreign power by permitting the FBI to issue an NSL not only when

⁶⁴ See S. REP. NO. 99-541, at 43-44 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3598-99. Indeed, Judge Marrero describes the addition as "inscrutable." See *Ashcroft*, 334 F. Supp. 2d at 482 n.34.

⁶⁵ Electronic Communication Privacy Act of 1986, Pub. L. No. 99-508 § 201, 100 Stat. 1848, 1867 (1986) (current version at 18 U.S.C. § 2709(b) (Supp. IV 2004)).

⁶⁶ *Id.*

⁶⁷ S. REP. NO. 99-541, at 44.

⁶⁸ S. REP. NO. 99-307, at 15.

⁶⁹ See *id.*

⁷⁰ See *id.*

⁷¹ See *id.* at 19.

the targeted individual was *himself* “a foreign agent or power,” but also when the target was anyone allegedly “*communicat[ing] with* foreign agents regarding terrorism or clandestine intelligence information.”⁷² The legislative history accompanying this amendment contains two particularly noteworthy statements. First, in lobbying for its request, the FBI gave a concrete description of a case in which the narrow scope of the NSL authority directly caused the loss of sensitive information.⁷³ Such content is notably absent from subsequent debates over the statutes. Second, in granting this narrow expansion, the House Judiciary Committee noted that the NSL is an “extraordinary device,” which is “[e]xempt from the judicial scrutiny normally required for compulsory process,” and as such, “[n]ew applications are disfavored.”⁷⁴ Interestingly, while granting this expansion, Congress also codified its belief that the Director’s authority to certify should be delegated only sparingly—the 1993 amendments explicitly require that such a designee must hold “a position not lower than Deputy Assistant Director.”⁷⁵

B. NSL Authority and the 2001 Patriot Act

The next major revision came in section 505 of the Patriot Act,⁷⁶ which relaxed both the “nexus” and certification requirements of § 2709 and its kindred provisions.⁷⁷ The Patriot Act eliminated the requirement of “articulable facts” showing a connection to a foreign power.⁷⁸ As a result, an FBI agent could (and still can) issue an NSL upon internal certification that the information sought is “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.”⁷⁹ In addition, section 505 added “Special Agent[s] in Charge in a Bureau field office” to the cate-

⁷² *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 482–83 (S.D.N.Y. 2004), *vacated and remanded sub nom. Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006).

⁷³ In the case mentioned, a caller, identifying himself only as an employee of the U.S. government, contacted a foreign embassy (whose phone lines were monitored), and offered to hand over “sensitive U.S. government information.” H.R. REP. NO. 103-46 at 2 (1993), *as reprinted in* 1993 U.S.C.C.A.N. 1913, 1914. Since this call only gave the FBI reason to believe that the caller was *volunteering* to be a foreign agent and not that he was in fact a foreign agent they could not use an NSL to trace the call. *Id.* Subsequently, the employee went on to surrender “highly sensitive information” to “representatives of the foreign nation.” *Id.*

⁷⁴ *Id.*

⁷⁵ Act of Nov. 17, 1993, Pub. L. No. 103-142, 107 Stat. 1491 (codified as amended at 18 U.S.C. § 2709(b) (Supp. IV 2004)).

⁷⁶ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S.C.).

⁷⁷ *See* 18 U.S.C. § 2709(b) (Supp. IV 2004).

⁷⁸ *See id.*; *supra* note 65 and accompanying text.

⁷⁹ 18 U.S.C. § 2709(b).

gory of FBI officials who could certify an NSL.⁸⁰ During the House Judiciary Committee's hearing on the Patriot Act, the need for such changes was described thus:

Because the NSLs require documentation of the facts supporting the "agent of a foreign power" predicate and because they require the signature of a high-ranking official at FBI headquarters, they often take months to be issued. This is in stark contrast to criminal subpoenas, which can be used to obtain the same information, and are issued rapidly at the local level. In many cases, counterintelligence and counterterrorism investigations suffer substantial delays while waiting for NSLs to be prepared, returned from headquarters, and served. The section [505 procedures] would streamline the process of obtaining NSL authority⁸¹

Several observations are in order regarding these dramatic changes and their attendant justifications. First, the grand jury subpoena analogy suggests that a counterterrorism agent should function much as a federal prosecutor does—if not, why labor to give them the same tools? But the agent's role in the post-9/11 FBI, where *preventing* terrorism is the top priority,⁸² is fundamentally different from that of a prosecutor, who generally strives to punish offenders *after* they have committed a crime. Given this new priority, it is worth considering whether experimenting with new types of process makes more sense than simply repurposing old ones.

Second, the legislative history of the Patriot Act never suggests that a more powerful and efficient FBI could be anything but an unmitigated good. Congress apparently did not consider potential costs of NSL proliferation, such as the risk of abuse or the financial burdens of compliance.⁸³ In the immediate aftermath of 9/11, this single-minded focus on efficiency is understandable. Six years later, however, Congress has shown little interest in revisiting the careful balancing it advocated when passing ECPA's NSL provisions in 1986.⁸⁴

Third, it bears noting which provisions of § 2709 have remained constant. Despite an extensive history of expansion and amendment, the language (and lack thereof) that courts and legislators found so troubling in 2004 and 2005 was already codified in the 1986 version of

⁸⁰ *Id.*

⁸¹ *Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the H. Comm. on the Judiciary*, 107th Cong. 57 (2001) (consultation draft), available at http://commdocs.house.gov/committees/judiciary/hju75288.000/hju75288_of.htm.

⁸² *See FBI Oversight: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 3 (2006) (statement of Sen. Edward M. Kennedy).

⁸³ *See, e.g.*, Paul Coggins, *It Doesn't Stay in Vegas*, RECORDER (San Francisco), Mar. 31, 2006, at 4 (discussing the abuses of NSL authority and the increased cost to businesses of complying with NSL requests).

⁸⁴ *See S. REP. NO. 99-307*, at 19 (1986).

§ 2709.⁸⁵ The NSL provision of ECPA makes compliance mandatory, but provides no mechanism for enforcement.⁸⁶ Similarly, the statute makes no mention of judicial review, and subsection (c) codifies the broad, enduring secrecy provision without mentioning enforcement.⁸⁷ Although Congress quickly drafted the Patriot Act amendments, the amendments did not in themselves make the NSL statutes unconstitutional. Rather, by enabling the FBI to issue exponentially more NSL demands, the amendments helped bring the statutes' constitutional infirmities to light.

Finally, the existence of an NSL "bottleneck"—the justification for the 2001 amendments—strongly suggests that NSLs had become something more than the "extraordinary" measures that legislators envisioned in 1993.⁸⁸ This Note next considers how this transformation occurred without any intervening legislative changes.

C. The Covert Expansion of 18 U.S.C. § 2709

Broadly speaking, NSL authority has five possible limits: who may certify the letter (the "certification" requirement); what they must certify (the "nexus" requirement); who may be served with a letter (the "subject" requirement); the type of information the target must disclose (the "scope" requirement); and how use of the authority is monitored (the "oversight" requirement).⁸⁹ Legislative amendments, culminating in section 505 of the Patriot Act, have greatly diminished the force of the first two limits—every FBI field office now has a supervisor authorized to issue NSLs,⁹⁰ and the relevance-to-a-terrorism-investigation nexus requirement is as low as that for a grand jury investigation.⁹¹

Meanwhile, technological change has drastically, albeit subtly, altered the "subject" and "scope" requirements of the statute. The growth of the Internet has vastly expanded the class of individuals and entities that can legitimately qualify as "electronic communications

⁸⁵ See *id.*

⁸⁶ See 18 U.S.C. § 2709(a) (2000) ("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." (emphasis added)).

⁸⁷ See *id.* § 2709(c) (current version at 18 U.S.C.A. § 2709(c) (Supp. 2006)) ("No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.").

⁸⁸ See H.R. REP. NO. 103-46, at 3 (1993), as reprinted in 1993 U.S.C.C.A.N. 1913, 1914.

⁸⁹ Congress and the agencies themselves regulate how the information obtained may be shared. They have done so in ways that are interesting and important, but beyond the scope of this Note.

⁹⁰ See *supra* note 80 and accompanying text.

⁹¹ See *supra* note 7.

service providers.”⁹² When Congress passed ECPA in 1986, this group of providers included a handful of telephone companies (since most computer-to-computer communications took place over phone lines) and a small number of “electronic mail compan[ies]” and “[e]lectronic ‘bulletin board[]’” operators.⁹³ The World Wide Web did not exist, and “electronic mail” was such a novel concept that ECPA’s drafters included an explanatory definition in the glossary of their report.⁹⁴ Today, such providers include not only commercial telephone companies and ISPs, but, according to the FBI, “any business or organization that enables users to send messages through a web site”—including universities, libraries, businesses, political organizations, and charities.⁹⁵

Simultaneously, the NSLs’ scope—the universe of information reasonably described as “subscriber information and toll billing records information, or electronic communication transactional records”⁹⁶—has exploded.⁹⁷ The statute does not define “electronic communications transactional records,” but the term, according to the FBI, includes, at a minimum, every Web site a particular person has accessed, as well as the recipient addresses and subject line of every e-mail sent through the provider in question.⁹⁸ Given the epochal increase since 1986 in both the sheer number of people using e-mail and the Internet and the ways in which they use it, the NSL statutes give FBI field agents subpoena power over a universe of information unimaginable to the ECPA’s drafters. Thus, it should come as no surprise that the FBI’s use of NSLs skyrocketed following the Patriot Act’s passage.⁹⁹ But because this change happened without legislative action, it is easy to overlook when considering how the NSL statutes have evolved. And it appears that Congress did overlook it, judging by both the legislative history surrounding 18 U.S.C. § 2709¹⁰⁰ and the reaction of individual legislators to the resultant legal battles over NSLs.¹⁰¹

⁹² 18 U.S.C. § 2709(a). The statute defines “electronic communication service” quite broadly: “any service which provides to users thereof the ability to send or receive wire or electronic communications.” *Id.* § 2510(15).

⁹³ See S. REP. NO. 99-541 at 8–9 (1986), as reprinted in 1986 U.S.C.C.A.N. 3562–63.

⁹⁴ See *id.*

⁹⁵ Memorandum in Support of Plaintiffs’ Motion for Summary Judgment, *ACLU, Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004) (No. 04 Civ. 2614), 2004 WL 2402699 (citation omitted) [hereinafter *ACLU Memorandum*] (“Thus, the FBI could use an NSL to obtain information from an advocacy organization such as the National Rifle Association or Moveon.org.”).

⁹⁶ See 18 U.S.C. § 2709(a).

⁹⁷ See *ACLU Memorandum*, *supra* note 95.

⁹⁸ See *id.*

⁹⁹ See *supra* text accompanying notes 6–10.

¹⁰⁰ See *supra* Part I.A.

¹⁰¹ See Gellman, *supra* note 8.

II

THE NSL CASES AND THE AMENDED PATRIOT ACT

A. *Doe v. Ashcroft*

The first legal challenge to the FBI's NSL authority under § 2709 arose in April of 2004,¹⁰² roughly eighteen years after Congress passed the legislation making NSL compliance mandatory.¹⁰³ In *Ashcroft*,¹⁰⁴ the American Civil Liberties Union (ACLU) and an anonymous ISP, who had received but not complied with an NSL, filed suit in the Southern District of New York.¹⁰⁵ They claimed that the statute, both facially and as applied, violated the ISP's First, Fourth, and Fifth Amendment rights.¹⁰⁶ The plaintiffs and the Government cross-moved for summary judgment, and Judge Victor Marrero awarded summary judgment for the plaintiffs in September 2004.¹⁰⁷

In his opinion, Judge Marrero first embarked on a thorough history of both § 2709 and other forms of compulsory process.¹⁰⁸ From the outset, the court observed that the statute, as drafted, forbade an NSL recipient from consulting with an attorney or any other party.¹⁰⁹ Furthermore, the statute did not permit any judicial review, either by a recipient's challenge or the Government's request for a judicial enforcement order.¹¹⁰ While acknowledging that the Fourth Amendment's "reasonableness" standard should be applied "permissive[ly]" to administrative subpoenas, Judge Marrero opined that the Constitution commands that the judiciary, and not the enforcing agency, be the ultimate arbiter of reasonability: "[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."¹¹¹ As a result, the court seemed inclined to hold that the statute violated the Fourth Amendment.

The Government urged the court to read into the statute provisions allowing judicial review and enforcement, arguing that, given the NSLs' similarities to administrative subpoenas, Congress clearly

¹⁰² See Am. Civil Liberties Union, Challenge to the "National Security Letter" Authority (Sept. 29, 2004), <http://www.aclu.org/safefree/patriot/17458res20040929.html>.

¹⁰³ Congress codified the NSL provisions of the ECPA and the amendments making RFPAs NSLs mandatory in 1986. See *supra* note 54 and accompanying text.

¹⁰⁴ 334 F. Supp. 2d 471 (S.D.N.Y. 2004), *vacated and remanded sub nom. Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006).

¹⁰⁵ *Id.* at 475.

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

¹⁰⁸ See *id.* at 480–91.

¹⁰⁹ See *id.* at 494.

¹¹⁰ See *id.*

¹¹¹ *Id.* at 495. However, Judge Marrero cited no cases supporting this assertion. See *infra* Part III.

envisioned judicial involvement in challenging and enforcing NSLs.¹¹² Further, the Supreme Court's doctrine of constitutional avoidance commanded an interpretation of § 2709 that would render it constitutional.¹¹³ The court declined to apply the doctrine, finding its use inappropriate where the problem is the statute's silence and not its use of ambiguous terms capable of either constitutional or unconstitutional interpretations.¹¹⁴ Additionally, the court was not willing to foreclose the possibility that, given the "sensitivity and overarching national priority associated with the purposes of the NSL statutes[,] . . . the absence of any reference to judicial review is the product of Congressional intent."¹¹⁵

Ultimately, however, the court decided that it need not decide the statute's facial compliance with the Fourth Amendment, since the statute clearly violated that provision as applied:

The crux of the problem is that the form NSL, like the one issued in this case, 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.¹¹⁶

In reaching this conclusion, Judge Marrero analogized to *Bantam Books, Inc. v. Sullivan*.¹¹⁷ In that case, the Supreme Court found that a Rhode Island administrative commission's similarly coercive practice violated the First Amendment.¹¹⁸ The commission sent "notices" to book distributors ordering them not to disseminate certain materials to minors and thanking them for their cooperation.¹¹⁹ In the words of Judge Marrero, the Supreme Court looked beyond the words of the letters to their "practical effect on a reasonable person"¹²⁰—the letters stifled *any* distribution of the material and thus effected an impermissible restraint on protected speech through "thinly veiled threats to institute criminal proceedings."¹²¹ Additionally, the Court reached its

¹¹² See *Ashcroft*, 334 F. Supp. 2d at 498.

¹¹³ See *id.* (quoting *INS v. St. Cyr*, 533 U.S. 289, 299–300 (2001) ("[I]f an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is fairly possible, [courts] are obligated to construe the statute to avoid such problems." (citation omitted))).

¹¹⁴ See *id.* at 499 (borrowing the phrase "sounds of silence" from SIMON & GARFUNKEL, *SOUNDS OF SILENCE* (Columbia Records 1966), to emphasize the importance of the law's silence to finding its meaning).

¹¹⁵ *Id.* at 500.

¹¹⁶ *Id.* at 501.

¹¹⁷ 372 U.S. 58 (1963).

¹¹⁸ See *id.* at 71–72.

¹¹⁹ *Id.* at 61–62.

¹²⁰ *Ashcroft*, 334 F. Supp. 2d at 503.

¹²¹ *Sullivan*, 372 U.S. at 68.

decision without addressing whether the Rhode Island statute authorizing the commission was itself unconstitutional.¹²²

Judge Marrero then addressed the First Amendment dimensions of § 2709(c), the statute's nondisclosure provision.¹²³ First, he held that the provision constituted a "prior restraint" on speech because it "prohibit[ed] speech before the speech occur[ed]."¹²⁴ Second, he held that § 2709(c) was a content-based restriction, not because it restricted a particular viewpoint, but because it foreclosed discussion on a particular topic entirely.¹²⁵ As a result, strict scrutiny applied.¹²⁶ Given the permanence of the provision's restraint and the fact that it applied to all persons affected in a given case, the court found § 2709(c)'s secrecy provision too broad to survive such scrutiny.¹²⁷

In conducting his tailoring analysis, Judge Marrero examined *Seattle Times Co. v. Rhinehart*¹²⁸ in detail.¹²⁹ In that case, a religious group's leader sued a newspaper that had run negative stories about the group.¹³⁰ The trial judge issued an order prohibiting the paper from publishing articles containing information it obtained via discovery.¹³¹ The Supreme Court upheld the order, arguing that it was properly tailored to further its interest in the secrecy of the proceedings because the litigant had no right to the information outside the context of litigation and because the order did not prevent the paper from publishing the same information if garnered by other means.¹³²

Judge Marrero then turned to *Butterworth v. Smith*,¹³³ a case in the *Rhinehart* line which probed the validity of a Florida statute extending the secrecy of grand jury proceedings beyond the expiration of the grand jury's term.¹³⁴ In *Butterworth*, a reporter serving as a grand jury witness sought to publish the contents of his grand jury testimony after the jury's term expired, a disclosure which the statute prohibited.¹³⁵ In holding the statute an invalid restraint on speech, the Court found two crucial factors that distinguished this case from *Rhinehart*: first, the secrecy interest was greatly diminished after the term expired because the need to prevent witness tampering or keep

¹²² See *id.* at 73–74 (Douglas, J., concurring); see also *Ashcroft*, 334 F. Supp. 2d at 505.

¹²³ See *Ashcroft*, 334 F. Supp. 2d at 511.

¹²⁴ *Id.* at 511–12.

¹²⁵ See *id.* at 512–13.

¹²⁶ See *id.* at 513.

¹²⁷ *Id.* at 514.

¹²⁸ 467 U.S. 20 (1984).

¹²⁹ See *Ashcroft*, 334 F. Supp. 2d at 516.

¹³⁰ *Rhinehart*, 467 U.S. at 22–23.

¹³¹ *Id.* at 25–26.

¹³² *Id.* at 36–37; see also *Ashcroft*, 334 F. Supp. 2d at 516.

¹³³ 494 U.S. 624 (1990).

¹³⁴ See *Ashcroft*, 334 F. Supp. 2d at 516–17.

¹³⁵ *Butterworth*, 494 U.S. at 626–28.

information from the target of the investigation had passed; and second, the statute restricted the dissemination of information that the reporter *already* possessed.¹³⁶

The Second Circuit further refined its approach to *Rhinehart* in *Kamasinski v. Judicial Review Council*.¹³⁷ That case involved a First Amendment challenge to Connecticut laws “mandating that judicial ethics proceedings be kept confidential unless and until the relevant administrative authorities determined that there was probable cause to believe that judicial misconduct had occurred.”¹³⁸ In rejecting the challenge, the court distinguished three different types of information involved: first, “the substance of an individual’s complaint or testimony”; second, “the complainant’s disclosure of the *fact* that a complaint was filed, or the witness’s disclosure of the *fact* that testimony was given”; and third, “information that an individual learns by interacting with” the other participants.¹³⁹ The Second Circuit decided that *Butterworth* addressed only the first type and that information of the latter two varieties could be subject to a “limited ban on disclosure” in light of the state’s interest in the secrecy of the misconduct proceedings.¹⁴⁰ Similarly, because the information covered by § 2709(c) arguably fell into the second *Kamasinski* category, the *Ashcroft* court felt that “some secrecy” surrounding the receipt of and compliance with an NSL “presumptively does little violence to First Amendment values.”¹⁴¹

However, as Judge Marrero observed, § 2709(c) went beyond the secrecy provisions upheld in *Rhinehart*, *Kamasinski*, and similar cases: the statute imposed “a *permanent* bar on disclosure in every case, making no distinction among competing relative public policy values over time, and containing no provision for lifting that bar when the circumstances that justify it may no longer warrant categorical secrecy.”¹⁴² The Government conceded that the statute provided no mechanism for lifting the secrecy requirement even though situations could arise where that requirement would not serve any conceivable state interest.¹⁴³

¹³⁶ *Id.* at 632–33 (holding that Florida could still enforce the part of the statute “which prohibits the witness from disclosing the testimony of *another* witness”).

¹³⁷ 44 F.3d 106 (2d Cir. 1994).

¹³⁸ *Ashcroft*, 334 F. Supp. 2d at 512.

¹³⁹ *Kamasinski*, 44 F.3d at 110.

¹⁴⁰ *Id.* at 111.

¹⁴¹ *Ashcroft*, 334 F. Supp. 2d at 519.

¹⁴² *Id.*

¹⁴³ *See id.* at 520 (“[A] case may arise in which the Government’s investigation has long since been completed and information about it has become public through Government sources or otherwise, in which the material obtained through an NSL revealed that there was no basis whatsoever to pursue the subject or target of the Government’s investigation, or in which the disclosure may have been made by a person in the chain of information,

The Government, however, advanced several arguments for the necessity of absolute secrecy. First, any less restrictive alternative would put investigators in an intolerable bind, requiring them to weigh the need for the desired information against the risk that a court would not provide the requisite secrecy each time they wished to issue an NSL.¹⁴⁴ Second, the Government pointed to a fundamental difference between “international terrorism and counterintelligence investigations” (where investigators can use NSLs) and investigations of “past crimes” (where investigators must rely on other forms of compulsory process).¹⁴⁵ Because the former type of investigation seeks to “uncover and disrupt *future* activities of typically large, long-term and expansive conspiracies” and because the desired end of such investigations is not necessarily a formal criminal trial, “the Government could theoretically have a much greater interest in continuing secrecy because certain elements of the investigation may remain in place for longer periods of time.”¹⁴⁶

The Government also advanced an argument, familiar from Freedom of Information Act disputes,¹⁴⁷ known as the “mosaic” theory.¹⁴⁸ As the Supreme Court has itself recognized, given the complexity and fluidity of international terrorism and intelligence investigations, evaluating the ramifications of an “isolated disclosure” proves incredibly difficult: “‘what may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context.’”¹⁴⁹ As a result, state actors should err on the side of continued secrecy when deciding whether to permit the disclosure of a given piece of information.¹⁵⁰

To buttress its mosaic argument, the Government referenced the relative competencies of the executive and judicial branches in determining how much secrecy a given situation requires.¹⁵¹ Because judges ordinarily “do not have national security expertise,” the judiciary, as an institution, lacks the ability “to understand the sensitivity of an isolated piece of information in the context of the entire intelli-

such as an employee or agent of the NSL recipient, who was not informed in any way of the secrecy requirement.”).

¹⁴⁴ See *id.* at 521.

¹⁴⁵ See *id.* at 522.

¹⁴⁶ *Id.* at 522–23.

¹⁴⁷ See, e.g., *CIA v. Sims*, 471 U.S. 159, 178 (1985).

¹⁴⁸ See *Ashcroft*, 334 F. Supp. 2d at 524 n.256 (quoting *Detroit Free Press v. Ashcroft*, 303 F.3d 681, 709 (6th Cir. 2002)); see also *Doe v. Gonzales*, 386 F. Supp. 2d 66, 77 n.9 (D. Conn. 2005), *dismissed as moot*, 449 F.3d 415 (2d Cir. 2006).

¹⁴⁹ *Ashcroft*, 334 F. Supp. 2d at 523 (quoting *Sims*, 471 U.S. at 178).

¹⁵⁰ See *id.*

¹⁵¹ See *id.*

gence apparatus.”¹⁵² As a result, the Supreme Court has acknowledged that the judiciary often owes “‘heightened deference to the judgments of the political branches with respect to matters of national security.’”¹⁵³

Although Judge Marrero acknowledged that such arguments justified *substantial* secrecy in cases involving NSL authority, he did not believe that they justified the *absolute* secrecy demanded by §2709(c):

[T]he Government cites no authority supporting the open-ended proposition that it may universally apply these general principles to impose perpetual secrecy upon an entire category of future cases whose details are unknown and whose particular twists and turns may not justify, for all time and all places, demanding unremitting concealment and imposing a disproportionate burden on free speech.¹⁵⁴

Notably, Judge Marrero did not opine on what a properly tailored confidentiality provision would look like, nor did he assert that judicial review would be essential to such a provision.¹⁵⁵ The Government, however, bears the burden of proving that a particular statute is sufficiently tailored: here, Judge Marrero held that “the Government has failed to carry its burden to show that the extraordinary scope of § 2709(c) is always necessary,” striking down § 2709 as unconstitutional under the First Amendment.¹⁵⁶

B. *Doe v. Gonzales*

Judge Marrero’s First Amendment concerns came into sharper focus in *Doe v. Gonzales*,¹⁵⁷ the second legal challenge to a § 2709 NSL. The plaintiffs here, again represented by the ACLU, filed suit on August 9, 2005, alleging that 18 U.S.C. § 2709(a), which authorized service of NSLs on any “wire or electronic communications service provider,” violated their First, Fourth, and Fifth Amendment rights.¹⁵⁸ Rather than moving immediately for summary judgment, the plaintiffs, desiring to participate fully in the escalating debate over the extension and amendment of the Patriot Act, sought a preliminary injunction barring enforcement of § 2709(c)’s nondisclosure provision.¹⁵⁹ Judge Janet Hall noted that a decision on the injunction

¹⁵² *Id.* (citing *N. Jersey Media Group v. Ashcroft*, 308 F.3d 198, 219 (3d Cir. 2002)).

¹⁵³ *Id.* at 523–24 (quoting *Zadvydas v. Davis*, 533 U.S. 678, 696 (2001)).

¹⁵⁴ *Id.* at 524.

¹⁵⁵ *See id.*

¹⁵⁶ *Id.* at 522. “Because the Court . . . granted Plaintiffs’ motion . . . on other grounds, [it] decline[d] to address Plaintiffs’ alternative argument that the statute violates the Fifth Amendment by failing to provide notice to persons to whom the records pertain.” *Id.* at 527 n.268.

¹⁵⁷ 386 F. Supp. 2d 66 (D. Conn. 2005), *dismissed as moot*, 449 F.3d 415 (2d Cir. 2006).

¹⁵⁸ *Id.* at 68–69 (quoting 18 U.S.C. § 2709(a) (2000)).

¹⁵⁹ *See id.* at 70.

could render a trial on the merits partially moot—once the plaintiffs could publicly disclose their identity in defiance of § 2709(c), there would be little point in litigating that provision’s constitutionality.¹⁶⁰ As a result, the plaintiffs needed to show a heightened likelihood of ultimate success on the merits.¹⁶¹ Accordingly, the decision strongly suggests Judge Hall’s view of the merits of the plaintiffs’ First Amendment claim.

Judge Hall found that the plaintiffs clearly demonstrated irreparable injury since the loss of a First Amendment right always engenders harm and at stake here was political speech relevant to “a current and lively debate” over the Patriot Act.¹⁶² The plaintiffs’ ability to speak out about NSLs generally and abstractly did not mitigate this loss since their ability to speak as a “known recipient of a[n] NSL” would have a much stronger rhetorical impact.¹⁶³

In determining the probability of the plaintiffs’ ultimate success, the court first had to determine the applicable level of scrutiny. Relying on *Bantam Books, Inc. v. Sullivan*,¹⁶⁴ Judge Hall found that the restriction created “‘coercion, persuasion and intimidation’” and thus served as a prior restraint.¹⁶⁵ The court also rejected the Government’s claim that § 2709(c) did not pose a prior restraint because the statute functioned like a gag order—it could only enforce compliance by a penalty after violation.¹⁶⁶ Judge Hall noted that the statute provided for no such penalty, a fact which the Government had conceded during oral argument.¹⁶⁷ She also found the provision to be a content-based restriction because it “‘has the potential for becoming a means of suppressing a particular point of view,’” namely “the view that certain federal investigative powers impose profoundly on individual civil liberties to the point that they violate our constitution.”¹⁶⁸ Thus, strict scrutiny applied, and the court had to determine whether the restraint was narrowly tailored to meet a compelling state interest.¹⁶⁹

¹⁶⁰ See *id.* at 82–83.

¹⁶¹ See *id.* at 71–72 (noting the need for showing irreparable injury and a clear or substantial likelihood of success on the merits).

¹⁶² *Id.* at 72.

¹⁶³ *Id.* at 73.

¹⁶⁴ 372 U.S. 58 (1963).

¹⁶⁵ *Gonzales*, 386 F. Supp. 2d at 74 (quoting *Sullivan*, 372 U.S. at 67).

¹⁶⁶ *Id.* at 74 n.5.

¹⁶⁷ *Id.* Judge Hall otherwise does not mention the lack of any enforcement mechanism for compliance with § 2709 NSLs.

¹⁶⁸ *Id.* at 75 (quoting *Forsyth County, Ga. v. Nationalist Movement*, 505 U.S. 123, 130–31 (1992)).

¹⁶⁹ *Id.*

The court pointedly refused to defer to the Government's findings of a compelling state interest¹⁷⁰ though the court did concur, based on *ex parte* review of classified materials, that the investigation clearly related to national security and that the NSL was not issued solely on the basis of activities protected by the First Amendment.¹⁷¹ This review, however, also "suggest[ed] strongly" that revealing the plaintiffs' identity would not harm the investigation.¹⁷² The court also rejected the Government's mosaic theory argument because the Government failed to prove the existence of a mosaic problem during oral argument and the plaintiff wished only to disclose information already obtained and did not desire access to previously unavailable material.¹⁷³

Addressing the tailoring question, the court followed *Ashcroft* in finding the secrecy provision overbroad due to its permanence.¹⁷⁴ It also noted that it was overbroad with regard to the *type* of information it restricted: "[a]ll details relating to the NSL."¹⁷⁵ Here the court pointed out that the Government did not object to publicly disclosing that Doe was "an organization with library records."¹⁷⁶ While the Government conceded that this disclosure would not harm its national security interest, such information clearly fell within § 2709(c)'s prohibition.¹⁷⁷

The court also rejected the Government's claim that the type of information barred here—the fact of an investigation—was indistinguishable from the information held to be the appropriate subject of a gag order in *Kamasinski*.¹⁷⁸ The court maintained that the information was substantively more similar to *Kamasinski*'s first category of information—the substance of an individual's complaint or testimony—since both involved a citizen's complaint about governmental action.¹⁷⁹ Here, the judge observed that the contested provision "creates a unique situation in which the only people who possess non-speculative facts about the reach of broad, federal investigatory authority are barred from discussing their experience with the pub-

¹⁷⁰ See *id.* at 76 (quoting *Hamdi v. Rumsfeld*, 542 U.S. 507, 536 (2004) ("[T]he United States Constitution . . . most assuredly envisions a role for all three branches when individual liberties are at stake.")).

¹⁷¹ *Id.* at 76.

¹⁷² *Id.* at 77.

¹⁷³ *Id.* at 78.

¹⁷⁴ *Id.* at 79–80 (citing *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 501–03 (S.D.N.Y. 2004), *vacated and remanded sub nom. Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006)).

¹⁷⁵ *Id.* at 80.

¹⁷⁶ *Id.*

¹⁷⁷ *Id.*

¹⁷⁸ *Id.* at 81–82.

¹⁷⁹ *Id.*

lic.”¹⁸⁰ Explicitly referencing former Attorney General Ashcroft’s “hysteria” speech,¹⁸¹ the court deemed this situation particularly noteworthy, given that advocates of the Patriot Act “have consistently relied on the public’s faith in the government to apply the statute narrowly in order to advocate for passage and reauthorization of various provisions” of the Act.¹⁸²

Accordingly, Judge Hall decided to order the injunction requested by the plaintiffs, but she also ordered a stay of the judgment pending appeal.¹⁸³ While noting that such a stay seemed logically inconsistent with granting an injunction in the first place, Judge Hall deemed it prudent to “permit the Court of Appeals an opportunity to consider an application for a stay pending an expedited appeal.”¹⁸⁴

Interestingly, although the *Ashcroft* plaintiff remained anonymous, the *Gonzales* plaintiff’s identity leaked fairly early in the proceedings. On September 2, less than a month after the anonymous plaintiff filed suit, the *New York Times* ran a story indicating that “John Doe” was actually Library Connection of Windsor, Connecticut, “a nonprofit consortium that serves 26 libraries in the Hartford area.”¹⁸⁵ It is unclear whether the Second Circuit took notice of this fact—on September 20, it granted the Government’s motion to extend the stay pending appeal of the injunction, given the risk of irreparable harm and injury to the public interest.¹⁸⁶ On October 7, the Supreme Court, with Justice Ginsburg sitting alone as Circuit Justice, denied the plaintiff’s emergency application to vacate the stay.¹⁸⁷

Justice Ginsburg’s brief, redacted opinion shows that she was mindful of this disclosure, noting that after Judge Hall’s decision, “the parties learned that, *through inadvertence, Doe’s identity had been publicly available for several days on the District Court’s Web site and on PACER* [an electronic public access docketing system] The parties also learned that *the media had correctly reported Doe’s identity on at least one occasion.*”¹⁸⁸ The opinion also suggests that she and the Second Circuit disagreed on whether this disclosure affected the validity of the

¹⁸⁰ *Id.* at 81.

¹⁸¹ *See supra* note 20 and accompanying text.

¹⁸² *Gonzales*, 386 F. Supp. 2d at 81.

¹⁸³ *Id.* at 82–83.

¹⁸⁴ *Id.* (citing *Rodriguez v. DeBuono*, 175 F.3d 227, 235 (2d Cir. 1999)).

¹⁸⁵ Alison Leigh Cowan, *Hartford Libraries Watch as U.S. Makes Demands*, N.Y. TIMES, Sept. 2, 2005, at B5.

¹⁸⁶ *Doe v. Gonzales*, 126 S. Ct. 1, 3 (2005), *ordered unsealed by and superseded by* 127 S. Ct. 1 (2005).

¹⁸⁷ *Id.* at 5.

¹⁸⁸ *Id.* at 4. The italicized text, redacted in the original opinion, became public in August 2006. *See* Press Release, Am. Civil Liberties Union, Supreme Court Unseals Documents in Patriot Act Case (Aug. 3, 2006), <http://www.aclu.org/safefree/nationalsecurityletters/26379prs20060803.html>.

stay. Justice Ginsburg mentioned the Second Circuit's decision that "additional circumstances . . . do not materially alter the balance of harms,"¹⁸⁹ but she ultimately decided that precedent and comity forbade interfering with the Second Circuit's deliberations merely because "a Circuit Justice disagrees" about the balance of harms.¹⁹⁰ She also noted that this mysterious new information created an anomaly: "Doe—the only entity in a position to impart a first-hand account of its experience—remains barred from revealing its identity, while others *who obtained knowledge of Doe's identity—when that cat was inadvertently let out of the bag—may speak freely on that subject.*"¹⁹¹

C. Congressional Response to the NSL Cases

As observed above, the 2006 amendments to the Patriot Act¹⁹² address the problems noted in *Gonzales* and *Ashcroft*.¹⁹³ The amendments explicitly allow an NSL recipient to consult with an attorney and challenge the letter in court—a judge may "modify or set aside the request if compliance would be unreasonable, oppressive, or otherwise unlawful."¹⁹⁴ The amendments also provide a mechanism for enforcing compliance by authorizing the Attorney General to petition for a court order compelling the recipient to comply with the request and by allowing the court to punish noncompliance with contempt sanctions.¹⁹⁵

In addition, the new legislation refines the nondisclosure provision in several ways. First, nondisclosure is no longer automatic: the official issuing the NSL must certify that disclosing the request "may result [in] a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person."¹⁹⁶ This bar excludes anyone who must be told in order to comply with the request, but the FBI Director or his designee can compel the recipient to identify "the person to whom such disclosure will be made or to whom such disclosure was made prior to the request," with the exception of any attorney consulted for advice about compliance.¹⁹⁷

¹⁸⁹ *Gonzales*, 126 S. Ct. at 4.

¹⁹⁰ *Id.* (citation omitted).

¹⁹¹ *Id.*; see *supra* note 188.

¹⁹² USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (codified as amended in scattered sections of the U.S.C.).

¹⁹³ See *supra* notes 28–34 and accompanying text.

¹⁹⁴ 18 U.S.C.A. § 3511(a) (Supp. 2006).

¹⁹⁵ *Id.* § 3511(c).

¹⁹⁶ *Id.* § 2709(c).

¹⁹⁷ *Id.* Congress added this mandatory identification requirement at the request of the Director of National Intelligence. See H.R. REP. NO. 109-333, at 95–96 (2005), as reprinted

The amendments also explicitly allow the recipient to challenge the nondisclosure requirement in court,¹⁹⁸ a change the committee described as a “clarifi[cation].”¹⁹⁹ If the recipient challenges the requirement within one year of the request, a high-ranking official may recertify the “[]danger” of disclosure, and the court must treat such certification as conclusive absent a showing of bad faith.²⁰⁰ The recipient may petition for disclosure once per year, but after the first year a lower-ranking official may make the conclusive recertification.²⁰¹ Finally, the amendments provide for criminal penalties if a recipient violates the secrecy provision “knowingly and with intent to obstruct an investigation or judicial proceeding.”²⁰²

The bill also makes some changes to the NSL statutes that the NSL cases did not discuss but that appear to be a response to the controversy surrounding those cases. First, the Attorney General must report, annually and publicly, regarding the number of requests for information concerning “different United States persons” made under the NSL statutes; however, requests for “subscriber information” under 18 U.S.C.A. § 2709 are excluded from this tally.²⁰³ Congress gives no explanation for this exception, but the drafters expressed a belief that news reports might overstate NSL statistics.²⁰⁴ The 2005 statistics, issued on Friday,²⁰⁵ April 28, 2006, stated that the FBI issued over 9,200 NSLs pertaining to roughly 3,500 citizens and legal residents during that year.²⁰⁶

In addition, the DOJ’s Inspector General must conduct an audit detailing the “specific functions and particular characteristics of the NSLs issued” and commenting on “the necessity of this law enforcement tool.”²⁰⁷ The first report on such an audit, published in March

in 2006 U.S.C.C.A.N. 184, 190, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_reports&docid=f:hr333.109.pdf.

¹⁹⁸ See 18 U.S.C.A. § 3511(b).

¹⁹⁹ H.R. REP. NO. 109-333, at 96.

²⁰⁰ 18 U.S.C.A. § 3511(b)(2). The “Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation” may make this certification. *Id.*

²⁰¹ *Id.* § 3511(b)(3). At this point, the designee of the FBI Director “in a position not lower than Deputy Assistant Director at Bureau Headquarters or a Special Agent in Charge in a Bureau field office” may make the recertification. *Id.*

²⁰² H.R. REP. NO. 109-333, at 96.

²⁰³ USA PATRIOT Improvement and Reauthorization Act of 2005 § 118(c)(1), Pub. L. 109-177, 120 Stat. 192, 218 (codified as amended in scattered sections of the U.S.C.).

²⁰⁴ See H.R. REP. NO. 109-333, at 97 (“Congress understands that current reporting may somewhat overstate the number of different U.S. persons about whom requests for information are made, because NSLs seeking information on a particular person may be served at different times and from different FBI field offices.”).

²⁰⁵ As any good reporter knows, Friday is the day when you release information you would prefer the public overlook.

²⁰⁶ Dan Eggen, *FBI Sought Data on Thousands in '05*, WASH. POST, May 2, 2006, at A4.

²⁰⁷ H.R. REP. NO. 109-333, at 97.

2007, cast doubt on the accuracy of the 2005 statistics by exposing “three flaws” in the way the FBI “records, forwards, and accounts for information about its use of NSLs.”²⁰⁸

III

A CRITIQUE OF THE AMENDED PATRIOT ACT

A. The Shortcomings of the NSL Debate

The courts’ primary concern in the NSL cases was *how* the FBI might use NSLs and not *what* might be obtained thereby. In the context of judicial review, this limited focus is perfectly understandable—the *Miller* line of cases seemingly resolved *what* the FBI could constitutionally obtain, eliminating the need for further scrutiny of this question.²⁰⁹ However, as the debate has shifted from the judicial to the legislative and political sphere, such limited scrutiny begins to seem shortsighted. Strangely, the need for a more comprehensive assessment of statutes like § 2709 has been obfuscated by the rhetoric of advocates, like the ALA, who are trying mightily to limit the NSL authority in other ways.²¹⁰

Consider *Gonzales*.²¹¹ For advocates like the ALA, the crucial fact is that the NSL recipient possessed “library records.”²¹² In their view, the worst case scenario is one where the FBI will use its various investigative powers to monitor the reading habits of the American public. In theory, such conduct puts the United States on a slippery slope toward an Orwellian dystopia where “thought police” jail citizens simply for reading subversive literature. Whatever the merits of this theory, it has tremendous popular resonance—indeed, section 215 of the Patriot Act has become known as the “library records” provision even though it does not explicitly mention libraries and allows the FBI to discover far more about a subject than what he or she has checked out of the library.²¹³

In reality, the government’s insatiable interest in the public’s reading habits rarely extends beyond the plots of Hollywood movies.²¹⁴ And although § 2709 is open to interpretation, no one has yet

²⁰⁸ NSL AUDIT, *supra* note 9, at xvi.

²⁰⁹ *See, e.g.*, 425 U.S. 435 (1976).

²¹⁰ *See, e.g.*, Press Release, Bernard Sanders, ACLU, American Library Association, Patriot Act Gag Order Press Conference (Sept. 28, 2005), <http://action.aclu.org/reformthepatriotact/legal/sanders.pdf>.

²¹¹ 386 F. Supp. 2d 66 (D. Conn. 2005).

²¹² *See id.* at 78 n.11.

²¹³ *See, e.g.*, Mike Allen, *House Votes to Curb Patriot Act*, WASH. POST, June 16, 2005, at A1.

²¹⁴ For example, take the 1995 movie *Se7en* (a.k.a. *Seven*):

DETECTIVE SOMERSET (Morgan Freeman): “For years, the FBI’s been hooked into the library system . . . monitoring reading habits . . . Books about on say, nuclear weapons, or *Mein Kampf*. Anyone who checks out a

argued that “electronic communications transactional records” could include a library’s lending records.²¹⁵ Indeed, since 2001, the NSL statutes have explicitly provided against the “thought police” scenario—the supervising agent must certify “that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution.”²¹⁶

The post-9/11 NSL “boom,” however, demonstrates that the FBI has a tremendous interest in whom its investigative targets e-mail and how those targets move money around—information that the FBI increasingly obtains through NSLs.²¹⁷ Thus, although NSL authority does affect libraries, it only does so to the extent that a library is a place where almost anyone can access the Internet in relative anonymity. Groups like the ALA obfuscate why this effect is still important by framing the debate in terms of *library* information, instead of *Internet* information.

B. The Amended NSL Statutes and Civil Liberties

From a civil libertarian perspective, the NSL amendments are problematic because they greatly enhance the compulsory power available to the FBI without a rational justification for such enhancement, a meaningful understanding of its dimensions, or effective safeguards against its abuse. The debate over its justification has proceeded with a complete lack of empirical evidence—the FBI has simply refused to divulge to Congress or the public information regarding the specifics on NSL usage, despite requests to do so.²¹⁸ Instead, the FBI has justified the changes by advancing abstract

flagged book has his library records fed to the FBI’s computers from then on”

DETECTIVE MILLS (Brad Pitt): “Wait, wait, wait . . . how is this legal?”

DETECTIVE SOMERSET: “Legal, illegal . . . these terms don’t apply. You can’t use the information directly, it’s just a useful guide. See it might sound silly, but you can’t get a library card without an ID and a current phone bill.”

SE7EN (New Line Cinema 1995). Interestingly, Somerset and Mills use the FBI list to track a villain named “John Doe.” *Id.* For another Hollywood conception of the FBI’s interest in popular reading habits, see CONSPIRACY THEORY (Warner Bros. 1997) (depicting a federal government that keeps tabs on a secret team of hrainwashed assassins by monitoring purchases of *The Catcher in the Rye*, a book the assassins are programmed to buy compulsively).

²¹⁵ Of course, assuming satisfaction of the relevance requirement, a grand jury subpoena or, after the Patriot Act, a FISA subpoena, could compel disclosure of such records. See *supra* note 37.

²¹⁶ 18 U.S.C. § 2709(b)(1) (Supp. IV 2004).

²¹⁷ See Eggen, *supra* note 206.

²¹⁸ See Gellman, *supra* note 8.

arguments of efficiency and parity under the rubric of harmonization.²¹⁹

The efficiency argument, while highly compelling—few would argue that the FBI should be less effective at detecting and preventing terrorism—is not unassailable. Heightened investigative efficiency has costs—in libertarian, economic, institutional, and other terms—that Congress must consider when shifting the balance of investigative power.²²⁰ But, without any empirical evidence on the utility of NSLs, such balancing is impossible.

Instead, the FBI simply argues that because federal prosecutors can use criminal subpoenas and, in analogous circumstances, other agencies can use administrative subpoenas, the FBI should have a comparable power.²²¹ Such an argument fails for several important reasons.

In the criminal context, the actors have very different institutional roles—the FBI agent investigates crimes, and the federal prosecutor prosecutes them. These different roles lead prosecutors and FBI special agents to respond to different incentives.²²² Nascent scholarship on the nature and effect of these divergent incentives suggests that prosecutorial control over compulsory process is more likely to prevent abuse.²²³ Thus, the prosecutor is seen as the “gatekeeper” to judicial process—in a criminal investigation, it is the prosecutor’s job to decide when to issue a subpoena, when to seek an order enforcing it, and when to bring charges.²²⁴

If this gatekeeping function curbs abuses of compulsory process, the NSL statutes diminish its efficacy. Because the FBI does not need to consult a prosecutor in order to issue an NSL, the statutes simply remove one of the three obstacles between the investigator and the judicial process, replacing this obstacle with a relevancy test that is virtually impossible to fail.²²⁵ In addition, as discussed in *Ashcroft*, counterterrorism investigations often do not have a criminal conviction as their logical endpoint.²²⁶ If there is no trial where illegally obtained evidence will be barred, agents have less incentive to obtain evidence legally.

²¹⁹ See *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 483–84 (S.D.N.Y. 2004), *vacated and remanded sub nom. Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006).

²²⁰ See *supra* note 83 and accompanying text.

²²¹ See Gellman, *supra* note 8.

²²² See Daniel Richman, *Prosecutors and Their Agents, Agents and Their Prosecutors*, 103 COLUM. L. REV. 749, 758 (2003).

²²³ See *id.* at 758–59.

²²⁴ See *id.*

²²⁵ See Gellman, *supra* note 8.

²²⁶ See *supra* note 146 and accompanying text.

Analogizing to administrative subpoenas presents similar problems. First, different agencies have different responsibilities; moreover, the powers they receive should be granted in accordance with those responsibilities, and not simply because another agency has them. Second, the argument improvidently assumes that the expansion of the administrative subpoena is an unmitigated good. The growth of the administrative subpoena has blurred the distinction between civil and criminal proceedings, giving agencies a counterpart to the grand jury subpoena in civil investigations and prosecutions.²²⁷ However, the invasiveness of grand jury power has traditionally been justified in the context of criminal investigations only—justified by society’s heightened interest in prosecuting crime and offset by the protections that the Bill of Rights grants to criminal defendants and by the nature of the grand jury as an independent and democratic body.²²⁸

In the civil context, the justifications offered must be, and have been, different.²²⁹ Often, the distinction is based on the subject’s “special relationship with the government.”²³⁰ Thus, the use of administrative subpoenas in, say, health care fraud investigations can partly be justified by noting that doctors receive a “privilege” from the state by engaging in licensed activities. This privilege is partly conditioned on a higher susceptibility to compulsory process.²³¹

The NSL authority applies in a third context: the realm of national security and counterterrorism.²³² The main problem with the parity and harmonization arguments²³³ is their faulty premise. To justify a given policy, parity must exist: A terrorism investigation must be substantially similar to either the “past crimes” investigations and prosecutions by federal prosecutors, or the civil investigations in which agencies deploy administrative subpoenas. Even the FBI, however, insists that investigations and prosecutions are different in significant ways.²³⁴ The secrecy of the investigation is far more important while actually obtaining a conviction is often far less important.²³⁵ And given the judiciary’s general lack of national security expertise, the use of judicial review to prevent abuse of compulsory process would be

²²⁷ See Graham Hughes, *Administrative Subpoenas and the Grand Jury: Converging Streams of Criminal and Civil Compulsory Process*, 47 VAND. L. REV. 573, 580 (1994).

²²⁸ See *id.* at 581–82.

²²⁹ See *id.* at 582.

²³⁰ *Id.*

²³¹ See *id.*

²³² See, e.g., Lauren M. Weiner, Comment, “Special” Delivery: Where Do National Security Letters Fit into the Fourth Amendment?, 33 FORDHAM URB. L.J. 1453, 1470 (2006).

²³³ See Gellman, *supra* note 8.

²³⁴ See, e.g., *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 522 (S.D.N.Y. 2004).

²³⁵ See *id.* at 523 (noting the importance of determining whether even isolated disclosures implicate national security).

less effective, or even counterproductive, than in the civil or criminal contexts.²³⁶ As a result, the new intrusions that the NSL authority represents—intrusions whose real significance is only beginning to be felt—must be justified on their own terms and not by analogizing to the realms of civil and criminal processes.

Such justifications are particularly important because the FBI wants more than just the expanded NSL authority. In a sense, the expanded NSL authority is simply a further slide down the slope toward a comprehensive administrative subpoena power for the FBI. The George W. Bush Administration has already lobbied for such power, and, in recent years, legislators have introduced bills that would confer it.²³⁷ Not surprisingly, the administration and legislators support such power with the same efficiency and parity arguments used in the NSL context. One Justice Department official, testifying before a Senate Subcommittee, called the lack of an FBI administrative subpoena “illogical,” an “anomaly” whose change would “level the playing field between terrorism investigations and other criminal investigations.”²³⁸ And advocates will undoubtedly use the expanded NSL statutes to argue for such a change—if the FBI has this power for one type of information, why not grant it for another?

This Note does not aim to discuss the merits of a more robust administrative subpoena power for the FBI. But the amended Patriot Act brings the FBI one step closer to that power. Thus far, the NSL debate has obscured this significant change rather than underscored it. When Congress passed the Patriot Act in 2001, it was aware that its actions could have unintended and adverse consequences. As a result, it included sunset and oversight requirements for some of the Act’s more radical provisions.²³⁹ The amendments to the NSL statutes had no sunset requirement, likely because Congress failed to apprehend the significance of those changes.²⁴⁰ By 2006, however, the importance of those changes was painfully obvious. Although Congress demanded an audit of the NSL authority, it failed to couple this oversight requirement with a sunset provision.²⁴¹ This regrettable omission sharply diminishes the likelihood that Congress will act to create

²³⁶ See *id.*

²³⁷ See Risa Berkower, Note, *Sliding Down a Slippery Slope? The Future Use of Administrative Subpoenas in Criminal Investigations*, 73 *FORDHAM L. REV.* 2251, 2271 (2005).

²³⁸ *Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists: Hearing Before the Subcomm. on Terrorism, Technology and Homeland Security of the S. Comm. on the Judiciary*, 108th Cong. 43–44 (2004) (statement of Rachel Brand, Principal Deputy Assistant Att’y Gen.), available at http://judiciary.senate.gov/testimony.cfm?id=1235&wit_id=3609.

²³⁹ See generally CHARLES DOYLE, AM. LAW DIV., CONG. RESEARCH SERV., *USA PATRIOT ACT SUNSET: PROVISIONS THAT EXPIRE ON DECEMBER 31, 2005* (2004), <http://www.fas.org/irp/crs/RL32186.pdf> (describing the Patriot Act sections that included sunset provisions).

²⁴⁰ See *id.*; *supra* Part I.B.

²⁴¹ See *supra* Part II.C.

a more efficient and benign NSL statute once it has the knowledge allowing it to do so. Instead, if the history described here is any guide, further increases in the FBI's compulsory power will come about not through deliberation, but by default.

C. How the Amended Patriot Act Hampers NSL Efficacy

The NSL cases indirectly raise a provocative question: Can Congress constitutionally create a form of compulsory process that differs substantially from a grand jury or administrative subpoena? In the 1980s, Congress apparently believed it could—the history of ECPA clearly demonstrates that Congress initially envisioned NSLs as an explicit alternative to the compulsory process of a subpoena; Article III courts were simply not to be involved.²⁴² Essentially, § 2709 allowed the FBI legally to demand information that ECPA otherwise protected.²⁴³ Such authority proved sufficient as long as the legality of the request was the only barrier to compliance. It seems, however, that this “alternative” process is exhausted once a recipient is unwilling to comply.

1. “Self-Help” as an Alternative to Contempt

Congress's solution is to allow the FBI to seek a court order punishing noncompliance with contempt proceedings.²⁴⁴ This is the same remedy relied on in the grand jury and administrative subpoena contexts. Although this is a remedy universally used, it is not the only effective remedy imaginable.

A form of judicially authorized “self-help” is another possibility: a judge could simply authorize the FBI to take the records to which, under the relevant NSL statute, it is legally entitled, rather than trying to force the NSL recipient to hand them over.²⁴⁵ For instance, a court might authorize the FBI to hack into the recipients' computers to obtain § 2709 electronic communications information.²⁴⁶ Such a “hacking warrant” would function less like a subpoena and more like a search warrant.

²⁴² See *supra* Part I.A.

²⁴³ See *id.*

²⁴⁴ See 18 U.S.C.A. § 3511(c) (Supp. 2006).

²⁴⁵ Most of the information that the FBI can compel via NSLs could alternatively be obtained, at least in theory, via computer hacking. This further emphasizes the novelty of the Fourth Amendment questions presented by such a form of compulsion.

²⁴⁶ The FBI has used hacking as a form of “self-help” in nondomestic computer crimes investigations. See, e.g., *United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001) (validating the FBI's use of a “sniffer” program, which allowed the FBI to obtain the suspect's password in a case involving international seizure of computer equipment).

Such a measure would make the NSL authority more effective in two ways. The first is obvious—in cases where the recipient is unwilling to comply, judicially authorized hacking makes unwillingness irrelevant. For some recipients, a contempt citation simply might not suffice to compel disclosure. A self-help remedy assures that such recalcitrance does not prevent the FBI from quickly obtaining important information.

Judicial authorization also increases the “threat value” of an NSL demand. The NSLs’ impressive track record suggests an obvious truth: recipients are more likely to comply with a demand if they feel they have little choice. A contempt remedy *creates* a choice—either hand the information over, or we will initiate proceedings that may result in a fine or jail time. A self-help remedy sharply *limits* choice—either hand the information over, or we will take it. Such a remedy would likely increase the number of recipients who comply initially, making the NSL demand more effective.

Would such a measure violate the Fourth Amendment? Generally, law enforcement may conduct such searches and seizures only with a warrant, based on a showing of probable cause—anything else is “unreasonable” and thus contrary to the Fourth Amendment.²⁴⁷ In exigent circumstances, however, the Supreme Court has approved conduct that is more intrusive or has based its approval on a reduced showing of cause.²⁴⁸ Most NSL information could be obtained via electronic hacking. And although the Fourth Amendment consequences of such a practice are uncertain, judicial authorization is arguably less intrusive than forced entry and physical seizure of property, which often accompany service of a search warrant.²⁴⁹

In addition, NSL requests generally occur in circumstances where the balance of interests strongly favors the government.²⁵⁰ The NSL recipient’s interest in the searched property—the records of a third party—is exceedingly low.²⁵¹ By contrast, the government’s interest in the information, given the national security dimensions of counterterrorism and counterintelligence investigations, is very high.²⁵² And, because a judge must issue an order to authorize self-help, *some* judi-

²⁴⁷ See, e.g., *United States v. Ventresca*, 380 U.S. 102 (1965).

²⁴⁸ See YALE KAMISAR ET AL., *MODERN CRIMINAL PROCEDURE: CASES, COMMENTS AND QUESTIONS* 358–63 (11th ed. 2005).

²⁴⁹ See generally David J.S. Ziff, Note, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841 (2005) (comparing computer searches to physical searches of property).

²⁵⁰ See *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 522 (S.D.N.Y. 2004), *vacated and remanded sub nom. Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006).

²⁵¹ See *id.* at 494 n.118.

²⁵² See *id.* at 511.

cial scrutiny would take place before the intrusion occurs, which is not the case in many other searches the courts have found reasonable.²⁵³

2. *How Much Judicial Review Is Enough?*

As *Gonzales* and *Ashcroft* observe, the most serious problem with 18 U.S.C. § 2709 and the other NSL statutes is that they create no mechanism for judicial review of NSL demands.²⁵⁴ This omission not only raises constitutional questions; it also hinders the statute's efficiency by making NSLs "empty threats"—the government is legally authorized to demand and receive certain information, but seemingly impotent when an NSL recipient refuses to provide it.

Again, Congress's solution replicates the procedures of other subpoenas.²⁵⁵ Such procedures almost certainly address the constitutional concerns in *Ashcroft* and *Gonzales*. However, Congress could have satisfied those concerns by providing far more limited review. Two potential problems are that the statutes allow recipients to *initiate* judicial proceedings and that they allow them to do so *immediately*.

a. *Must an NSL Recipient Be Allowed to Initiate Judicial Review?*

Under the amended Patriot Act, a petitioner may challenge an NSL upon receipt, just like one may challenge a grand jury subpoena.²⁵⁶ What if the recipient could challenge the reasonability of the request only if and when the FBI initiated proceedings to compel compliance?

Because, historically, the vast majority of NSL recipients comply without challenge,²⁵⁷ this difference may seem insignificant. It bears repeating, however, that the fact of near-universal NSL compliance seems to result from the apparent lack of choice such demands provide.²⁵⁸ The fewer legitimate alternatives to compliance a recipient has, the more likely the recipient is to comply.

The difference also matters because an investigating agent has two competing concerns. The agent wants to obtain the documents, but he also wants to preserve the secrecy of the investigation. As *Gonzales* vividly demonstrates, any judicial proceeding threatens that secrecy.²⁵⁹ Ideally, the agent should be able to serve the request and bar

²⁵³ See KAMISAR, *supra* note 248, at 316–17.

²⁵⁴ See *supra* Part II.A–B.

²⁵⁵ See *supra* Part II.C.

²⁵⁶ See *supra* note 194.

²⁵⁷ Cf. *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 481 (S.D.N.Y. 2004), *vacated and remanded sub nom. Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006) (noting that, even before the ECPA, "the FBI had been issuing non-mandatory NSLs to communications providers, who, in most cases, complied voluntarily").

²⁵⁸ See *supra* Part III.C.1.

²⁵⁹ See *supra* Part II.B.

even a noncompliant recipient from disclosure. The agent could then decide whether to bring suit to compel compliance (increasing the risk that sensitive information will leak out) or to forego litigation and try to obtain the information through other means. Thus, such a small change would allow the government to postpone the Hobson's choice that it faces when seeking to compel compliance with an NSL—forego the information or risk disclosing sensitive information by initiating judicial process.²⁶⁰

Such a change might pose Fourth Amendment problems. However, it is not clear whether Fourth Amendment "reasonability" requires any mechanism for review. In *Ashcroft*, Judge Marrero suggests that it does, noting that even an empty threat of self-help would be unreasonable under the Fourth Amendment.²⁶¹ Although Congress apparently took him at his word, the contention that the Fourth Amendment requires judicial review constitutes the most tenuous part of the *Ashcroft* opinion.

First, Judge Marrero suggests that a search or seizure authorized without the possibility of judicial review is *de facto* unreasonable under the Fourth Amendment.²⁶² However, he offers no Supreme Court or Second Circuit law to support this claim.²⁶³ He also argues that, as applied, the combination of secrecy and lack of judicial oversight in the NSL process creates implied coercion and causes recipients improperly to "forfeit" their Fourth Amendment freedom from unreasonable seizures.²⁶⁴ Simply put, because there was no possibility of review and because automatic, perpetual secrecy was required, the NSL demand in *Ashcroft* was unreasonable and thus violated the Fourth Amendment.²⁶⁵ Assuming *arguendo* the truth of this proposition, it does not foreclose the possibility of a constitutionally reasonable mix of secrecy and judicial review that still provides less review than other forms of compulsory process.

In addition, Judge Marrero's contention that implied coercion can violate the Fourth Amendment is quite novel. Finding no Fourth Amendment case law on point, he analogizes to a single Supreme Court case which found that a similarly coercive practice violated a victim's First Amendment rights.²⁶⁶

²⁶⁰ See *Ashcroft*, 334 F. Supp. 2d at 521.

²⁶¹ See *id.* at 496.

²⁶² See *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.").

²⁶³ See *id.*

²⁶⁴ See *id.* at 506.

²⁶⁵ See *id.*

²⁶⁶ See *id.* at 505-06.

The courts, however, do not enforce all constitutional rights identically. Perhaps a more apposite comparison would be the Fifth Amendment right against self-incrimination or the right to counsel, where accusations of coercion or trickery are more common. In the *Miranda*²⁶⁷ and *Edwards*²⁶⁸ line of cases, the Supreme Court has often upheld police practices at least as coercive as those involved in serving an NSL, causing “reasonable” suspects to forfeit their rights even where they are not required to do so and where such forfeiture is emphatically against their interest.²⁶⁹ Likewise, the FBI may be able to convince a recipient to forego judicial review without violating that individual’s constitutional rights. Under the case law which Judge Marrero cites, forbidding the recipient from challenging a particular demand only becomes unreasonable when the court is attempting to punish the recipient for disobeying it.²⁷⁰

b. *When and How Must Nondisclosure Be Reviewed?*

Of course, the Fourth Amendment is not the only constitutional provision that the NSL statutes implicate. Indeed, given § 2709’s broad nondisclosure provisions, the *Ashcroft* and *Gonzales* courts found the First Amendment problems even more troubling.²⁷¹ Assuming that less review makes the NSL authority more powerful, it is instructive to gauge how much judicial review of a nondisclosure provision would satisfy the courts’ First Amendment concerns.

The answer could be none at all. Neither *Ashcroft* nor *Gonzales* requires judicial review to *impose* a nondisclosure requirement.²⁷² Indeed, both courts were inclined to give the Government *tremendous* amounts of latitude—it seems the only thing they could not stomach was an automatic, perpetual nondisclosure provision.²⁷³ Unfortunately, that is just what § 2709 seemed to demand. Suppose the statute merely required certification of the need for secrecy and allowed a recipient to challenge that need after six months. Even a provision allowing disclosure at the Bureau’s discretion or after a period of five or ten years would be far more tailored than the current statute. Given the potential enormity of the state interest and the minimal value of the prohibited speech, many judges would likely not strike down the statute on First Amendment grounds. In this sense, the 2006 amendments might go too far in allowing an automatic challenge immediately upon receipt of an NSL.

267 *Miranda v. Arizona*, 384 U.S. 436 (1966).

268 *United States v. Edwards*, 415 U.S. 800 (1974).

269 See KAMISAR, *supra* note 248, at 715 (collecting and summarizing cases).

270 See *supra* notes 120–121.

271 See *supra* Part II.A–B.

272 See *id.*

273 See *id.*

Thus, the Supreme Court might have found that the Constitution requires less judicial oversight than the current statute provides. This discrepancy should trouble those who feel that the executive branch's antiterrorism tools should be as powerful as possible. In some cases, a recipient's ability to seek judicial review could delay the acquisition of valuable information and increases the risk of inadvertent disclosure of sensitive information. This might be too high a price to pay for a level of judicial review that many commentators feel is merely "cosmetic."²⁷⁴

CONCLUSION: HARMONIZATION OR DISCORD?

By expanding the NSL authority in the Patriot Act, Congress gave the FBI the power of compulsory process over a vast and expanding universe of information. As a result, the NSL, initially employed only in extraordinary situations, has become a routine investigative tool. The astonishing number of NSLs issued by the Bureau in the wake of the Patriot Act ensured that someone would eventually challenge the use of this tool. As soon as someone did, the NSL statutory scheme collapsed. Because the statutes absolutely barred disclosure and provided no mechanism for review or reinforcement, federal courts struck down § 2709 as an unconstitutional empty threat. In response, Congress amended the statute to create a constitutional form of NSL authority. In this, they seem to have succeeded.

However, in the rush to remedy the NSL statutes' constitutional defects, Congress has failed to ask two critical questions. First, is the NSL authority still necessary? Second, assuming it is, how can it be made as effective as possible?

Answering the first question involves a frank appraisal of the NSL's effect on civil liberties. It requires Congress to explain—in language less vague than that employed by ECPA in 1986 and still relied on today—the types of information that the FBI can use NSLs to demand. It requires Congress to acknowledge that the FBI is not the same as the Securities and Exchange Commission and that a special agent is not the same as a federal prosecutor and then to explain why, despite these differences, the FBI should have comparable compulsory power. It requires some indication that Congress understands how NSLs work, and is thus capable of deciding that the need for such a tool justifies the increased intrusions that tool engenders.

Answering the second question requires Congress to reject the Panglossian notion that the current forms of compulsory process are the best forms possible. This notion, a fundamental premise of the "harmonization" argument, is particularly absurd in the context of the

²⁷⁴ See, e.g., Editorial, *Patriot Act Cosmetics*, ST. PETERSBURG TIMES, Mar. 10, 2006, at 14A.

Patriot Act. If anything, the 9/11 attacks dramatically demonstrated the shortcomings of the investigative tools and procedures that constitute the status quo.

Insisting on “harmonization” hinders both inquiries. “Harmonization” is the fallacy that because one process functions a certain way, a related process must function similarly. The inquiries are also hindered by a glaring lack of information about how the FBI actually uses NSLs.

This lack of information makes a constructive debate over the proper contours of the NSL authority impossible. It also points to the most blatant shortcoming in the current NSL statutes—the lack of any sunset provision.

To be fair, Congress has demanded an audit of the NSL authority. But it is simply unwise to first grant the FBI a tremendous power and then expect them to justify the need for it. Without a sunset provision, there’s no apparent penalty if the FBI simply refuses—as it has in the past—to comply with Congress’s request for information. Ironically, it seems that Congress—just as it did in 1986—has authorized a threat without providing a way to back it up. The difference is that now—after the furor surrounding the NSL statutes—Congress should know better.

