OKLAHOMA CITY UNIVERSITY
LAW REVIEW

VOLUME 33 SUMMER 2008 NUMBER 2

ARTICLES

THE CHAINS OF THE CONSTITUTION AND LEGAL PROCESS IN THE LIBRARY: A POST-USA PATRIOT REAUTHORIZATION ACT ASSESSMENT

Susan Nevelow Mart*

"In questions of power, then, let no more be heard of confidence in man, but bind him down from mischief by the chains of the Constitution."[1]

The forms of legal process[2] authorized by the USA PATRIOT Act,[3] as they apply to library patron information, implicate both First Amendment and Fourth Amendment values.[4] Seizing evidence of what a

* Faculty Services Librarian and Adjunct Professor of Law, UC Hastings College of the Law, San Francisco, California. This paper is based in part on a presentation given by the author at the 100th Annual Meeting of the American Association of Law Libraries, New Orleans, July 17, 2007. The author would like to acknowledge the contributions to this subject made by the writings of Lee Strickland.

1. Thomas Jefferson, Draft of the Kentucky Resolutions, *in* THE POLITICAL WRITINGS OF THOMAS JEFFERSON 156, 161 (Edward Dumbauld ed., 16th prtg. 1982).

2. Legal process is a generic term for a court order to produce documents or information. *Cf.* BLACK'S LAW DICTIONARY 1242 (8th ed. 2004) ("Process validly issued.").

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

4. Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1055 (Colo. 2002).

person is thinking about by looking at what he or she is reading or perusing on the Internet is inimical to both of these tenets of the Bill of Rights. Librarians have been among the strongest critics of the USA PATRIOT Act's incursions into this realm of intellectual freedom. And the government has heaped scorn on librarians for their opposition.[5] But librarians do not oppose law enforcement's legitimate efforts to fight terrorism through the use of legal process in libraries; what librarians oppose is government fishing expeditions directed at the content of what people read or access in the library. There is a balance that can easily be maintained between law enforcement's access to library records and the protection of library patrons' civil liberties. The USA PATRIOT Act upsets that balance.

The use of legal process to access library records is not new. In the 1980s, the legislative response to government programs like the Library Awareness Program,[6] which sought the help of librarians in reporting "suspicious" readers of unclassified information, was the passage of state statutory protection for library records.[7] Although the statutes vary widely in their specificity, most do make an exception for libraries to provide records pursuant to a court order.[8] The judicial review requirement for court orders assures that overly broad requests for library records will not be issued—that there is, in fact, a constitutionally sufficient nexus between a specific crime and a specific library user.[9]

---

5. *See, e.g.*, John Ashcroft, U.S. Attorney Gen., Protecting Life and Liberty, Remarks in Memphis, Tenn. (Sept. 18, 2003), http://www.usdoj.gov/archive/ag/speeches/2003/091803memphisremarks.htm; Eric Lichtblau, *At F.B.I., Frustration Over Limits on an Antiterror Law*, N.Y. TIMES, Dec. 11, 2005, at A48 ("'While radical militant librarians kick us around, true terrorists benefit from OIPR's failure to let us use the tools given to us.'").

6. HERBERT N. FOERSTEL, SURVEILLANCE IN THE STACKS: THE FBI'S LIBRARY AWARENESS PROGRAM 10-12 (1991) (describing the Library Awareness Program's attempt to monitor the reading habits of suspicious and foreign-looking patrons in more detail).

7. *See id.* at 133–34; State Laws on the Confidentiality of Library Records, http://www.library.cmu.edu/People/neuhaus/state_laws.html (last visited Oct. 5, 2008). All but two states have statutes expressly protecting library records; the two states without statutes (Kentucky and Hawai'i) have opinions from their attorneys general that library records are confidential. MARY MINOW & TOMAS A. LIPINSKI, THE LIBRARY'S LEGAL ANSWER BOOK 200–10 (2003).

8. MINOW & LIPINSKI, *supra* note 7, at 200-10.

9. Where the government seeks to discover library records because of the *content* of what a patron has read or viewed, the First Amendment requires the strictest scrutiny before any legal process can issue. *Tattered Cover*, 44 P.3d at 1059.

> The chilling effect that results from disclosure of customer purchase records

With most court-issued orders, because a library is being asked to produce records,[10] there is an opportunity to consult with an attorney before compliance.[11] Libraries are not required to—and may violate state law if they do—turn over library records in response to overbroad, improperly issued, or unconstitutional requests for patron records.[12]

The passage of the USA PATRIOT Act changed the landscape of legal process in the library. The debate about the USA PATRIOT Act has been public, vehement, and well documented;[13] but the outcry has diminished since the passage of the USA PATRIOT Reauthorization Acts.[14] This article will discuss the various forms of post-USA

> occurs because of the general fear of the public that, if the government discovers which books it purchases and reads, negative consequences may follow. However, if the government seeks a purchase record to prove a fact unrelated to the content or ideas of the book, then the public's right to read and access these protected materials is chilled less than if the government seeks to discover the contents of the books a customer has purchased.

Id.

10. *See generally* Lee S. Strickland, Mary Minow & Thomas Lipinski, *Patriot in the Library: Management Approaches When Demands for Information Are Received From Law Enforcement and Intelligence Agents*, 30 J.C. & U.L. 363, 379 (2004).

11. Although search warrants are immediately executable, there is a penalty for overbroad or improper search warrants: suppression of the evidence gathered pursuant to the tainted warrant. This is basic Fourth Amendment law.

> If an unreasonable search has been made in violation of the Fourth Amendment, it is not merely the material seized that cannot be admitted in evidence. The government may not use the information thus improperly gained as a means of finding proper evidence. In what the Court has rightly called "a time-worn metaphor," the government is said to be barred from use of "a fruit of the poisonous tree."

3A CHARLES ALAN WRIGHT, NANCY J. KING & SUSAN R. KLEIN, FEDERAL PRACTICE AND PROCEDURE § 677 (3rd ed. 2004) (footnotes omitted) (quoting Harrison v. United States, 392 U.S. 219, 222 (1968); Nardone v. United States, 308 U.S. 338, 341 (1939)).

12. *See, e.g.*, Lee S. Strickland, *Responding to Judicial Process: A Guide to the Unexpected for Search Warrants, Subpoenas and Otherwise*, 49 VA. LIBR., Spring 2003, http://scholar.lib.vt.edu/ejournals/VALib/v49_n1/strickland.html.

13. A search for "PATRIOT Act" in the same paragraph as "libraries" in Westlaw's "Journals and Law Reviews" database brings up 139 results. The same search in Lexis' "Law Reviews and Journals" database brings up 275 results. Comparable news searches were terminated for bringing up too many results. The searches were performed on October 2, 2007. The public outcry about section 215 has been judicially noted. *See* ACLU v. U.S. Dep't of Justice (*ACLU II*), 321 F. Supp. 2d 24, 32 (D.D.C. 2004).

14. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006) (codified in scattered sections of U.S.C.); USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, 120 Stat. 278 (codified in scattered sections of U.S.C.).

PATRIOT Act process, how those forms of process have been amended by the Reauthorization Acts, and what areas for public debate and concern still remain. Librarians have been enormously successful advocates against portions of the USA PATRIOT Act,[15] but there are many statutory problems affecting civil liberties that still need to be addressed. There is still plenty of opportunity for advocacy.

I. SECTION 215—THE LIBRARY PROVISION

The original focus of the debate for librarians was section 215.[16] It is fair to say that the library community became section 215's most outspoken opponent; the section began to be called the "library provision."[17] The USA PATRIOT Act changed the type of business records that could be requested from the Foreign Intelligence Surveillance Court ("FISC"), from transportation-related business records to the records of any business—including libraries.[18] The pre-USA PATRIOT Act section concerning records that could be requested from the FISC clearly had no affect on libraries.[19] Almost everyone was surprised to discover there even *was* a secret foreign-intelligence court.

Section 215 included a permanent and extremely broad gag order, precluded consultation with an attorney, and contained no provisions for review of the gag order.[20] Section 215 allowed government fishing expeditions for information from physical library records such as circulation records or internet-use sign-up sheets, or for information concerning computer search histories from library computers or servers, and the library community responded in force.[21]

15. *See* section 215 audit report discussion *infra* p. 446-47.

16. USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287-88 (codified at 50 U.S.C §§ 1861-1863 (Supp. I 2001)).

17. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS 8-9 (2007) [hereinafter SECTION 215 AUDIT REPORT], http://www.usdoj.gov/oig/special/ s0703a/final.pdf.

18. 50 U.S.C. § 1861 (Supp. I 2001).

19. 50 U.S.C. § 1862(a) (2000).

20. *See* 50 U.S.C. §§ 1861(d), 1862 (Supp. I 2001).

21. *See supra* note 13 and accompanying text.

II. SECTION 215 WAS SUBSTANTIALLY CHANGED BY THE REAUTHORIZATION ACT

One complaint raised about section 215 orders was that the orders need not be directed at a particular person. Critics of the section wanted to return to pre-USA PATRIOT Act standards for issuing an order, which required that the order be about a specific person who is strongly suspected of terrorism,[22] instead of the post-USA PATRIOT Act standard "that the records concerned are sought for an authorized investigation."[23] Although the Senate version of the Reauthorization Act did contain language requiring more particularized statements regarding the target of the order,[24] the compromise language that actually passed only added a weak relevancy standard: the records have to be "relevant to an authorized investigation."[25] The records are "*presumptively relevant*" if they pertain to "an agent of a foreign power," "a suspected agent," or "an individual in contact with" a suspected agent.[26] Under this broad standard, it is not hard for the government to assert relevancy.

Section 215's original non-disclosure requirement was stringent: "No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation [("FBI")] has sought or obtained tangible things under this section."[27] The language precluded the right to consult an attorney, since an attorney is rarely the "person[] necessary to produce the tangible things."[28] The USA PATRIOT Improvement and Reauthorization Act of 2005 ("Reauthorization Act I") addressed this

22. 50 U.S.C. § 1862(b)(2)(B) (2000) (requiring, in an application for access to records, that "there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power").

23. 50 U.S.C. § 1861(b)(2) (Supp. II 2002).

24. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, S. 1389, 109th Cong. § 7 (as reported by Senate, July 22, 2005). The Senate-passed version of USA PATRIOT Improvement and Reauthorization Act of 2005 required that the statement of facts show that the records or things sought are relevant to an authorized investigation *and* that the things sought pertain to, or are relevant to the activities of, a foreign power or agent of foreign power, or pertain to an individual in contact with or known to a suspected agent of a foreign power. *Id.*

25. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192, 196 (2006) (codified at 50 U.S.C.A. § 1861(b)(2)(A) (West Supp. 2008)).

26. *Id.* (emphasis added).

27. 50 U.S.C. § 1861(d) (Supp. II 2002).

28. *Id.*

problem, and the recipient of a FISC order for business records is now expressly authorized to consult with an attorney to obtain legal advice about the order.[29] The recipient does not have to disclose the attorney's name to the FBI, but, if asked, must inform the FBI who else knows of, or will know of, the order.[30]

The Reauthorization Act I added judicial review provisions for section 215 orders by FISC judges.[31] If the judge determines that the petition for review is "not frivolous," the judge has discretion to set aside or modify an order to produce documents "only if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful."[32] So the order cannot be modified because it is onerous, oppressive, or overbroad. The non-disclosure requirement cannot be challenged until a year after the order to produce has been issued.[33] However, once the one-year moratorium is over, the recipient can file a petition to modify or set aside the non-disclosure requirement; a FISC judge must initially determine whether or not the petition is frivolous.[34] If the petition is not frivolous, the court must promptly hear the petition, but can grant the order "only if the judge finds that there is no reason to believe that disclosure may *endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.*"[35] If the government certifies that there is a reason to believe "that disclosure may endanger the national security of the United States or interfere with diplomatic relations," the certification is *conclusive* "unless the judge finds . . . the certification was made in bad faith," and the recipient is then bound by the gag order for another year.[36]

29. USA PATRIOT Improvement and Reauthorization Act § 106(e), 120 Stat. at 197 (codified at 50 U.S.C.A. § 1861(d)(1)(B) (West Supp. 2008)).

30. USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, § 4, 120 Stat. 278, 280 (codified at 50 U.S.C.A. § 1861(d)(2)(C) (West Supp. 2008)).

31. USA PATRIOT Improvement and Reauthorization Act §106(f)(2), 120 Stat. at 198 (codified at 50 U.S.C.A. § 1861(f) (West Supp. 2008)). Review of a petition challenging a section 215 order shall be conducted *in camera*. *Id.*

32. *Id.* (codified as amended at 50 U.S.C. § 1861(f)(2)(B) (West Supp. 2008)).

33. USA PATRIOT Act Additional Reauthorizing Amendments Act § 3, 120 Stat. at 278-79 (codified at 50 U.S.C.A. § 1861 (West Supp. 2008)).

34. *Id.*

35. *Id.* (emphasis added).

36. *Id.*

There are serious constitutional problems with this scenario. The gag order imposes a prior restraint of speech about even the most generic details of the order: no recipient can discuss the mere fact that an order was received or debate the fact that the order appeared to be a fishing expedition of the sort that, during debates on the USA PATRIOT Act, the government consistently denied it ever engaged in.[37] Nor can the recipient discuss the profound effect the gag order has had on the recipient's business or personal life.[38] The gag order also applies in criminal investigations or where the safety of any person is an issue, so national security need not even be implicated to require the continuation of the order.[39] In invalidating a similar[40] non-disclosure provision imposed on recipients of national-security letters ("NSL"), a district court stated the following:

> To the contrary, NSL recipients are effectively barred from engaging in any discussion regarding their experiences and opinions related to the government's use of NSLs. For example, an NSL recipient cannot communicate to anyone indefinitely that it received an NSL, the identity of the target, the type of information that was requested and/or provided, general statistical information such as the number of NSLs it received in

---

37. *See, e.g.*, Ashcroft, *supra* note 5 ("[T]he 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."); Alberto R. Gonzales, *Reauthorize the Patriot Act: Congress Should Reauthorize the Patriot Act and Further Strengthen Homeland Security*, WASH. POST, Dec. 14, 2005, at A29.

38. *Responding to the Inspector General's Findings of Improper Use of National Security Letters by the FBI: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 110th Cong. 27-35 (2007) [hereinafter *Hearing*] (statement of George Christian, Executive Director, American Library Association).

39. USA PATRIOT Act Additional Reauthorizing Amendments Act § 3, 120 Stat. at 278-79 (codified at 50 U.S.C.A. § 1861 (West Supp. 2008)).

40. Although there are substantive differences between the two non-disclosure provisions (*see* discussion *infra* pp. 461-63 for a more detailed review of the non-disclosure provisions for NSLs), none of those differences militate in favor of the constitutionality of section 215. The two main differences are that NSL recipients do not have to wait for a year to challenge the non-disclosure order, and that the imposition of the non-disclosure order is not automatic. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 116(a), 120 Stat. 192, 213-14 (codified at 18 U.S.C.A. § 2709(c) (West Supp. 2008)), *invalidated by* Doe v. Gonzales (*Doe III*), 500 F. Supp. 2d 379 (S.D.N.Y. 2007); *Id.* § 115, 120 Stat. at 211-13 (codified at 18 U.S.C.A. § 3511 (West Supp. 2008)), *invalidated in part by Doe III*, 500 F. Supp. 2d 379.

> the previous month or year, its opinion as to whether a particular NSL was properly issued in accordance with the applicable criteria, or perhaps even its opinion about the use of NSLs generally (*e.g.*, whether NSLs are being used legitimately, whether their use may be stifling speech, whether the government may be abusing its power under the statute, etc.).[41]

Another problem with the review procedure is that, in the absence of overt bad faith, the court is absolutely bound by the government's certification.[42] In the context of NSLs, one court found that such a constraint on judicial review of legislation affecting the First Amendment to be so severe, that it violated the constitutional provisions of checks and balances and separation of powers.[43] Critics of this section wanted review of section 215 orders in the federal district courts.[44] Access to the federal courts is simpler, and the court procedures are more familiar, which might broaden the base of lawyers willing to appear in a hearing challenging a section 215 order.

The final version of the Reauthorization Act I did not exempt libraries and bookstores from section 215, but it did address some of the issues raised by the library community. Now, only three of the FBI's highest-level employees have the authority to make an application to the FISC for "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person."[45] Because of the controversy about the use of section 215 to procure library records, a section 215 order has *never*, according to the Office of the Inspector General ("OIG"), been issued to request the production of library records.[46] The Reauthorization Act I

41. *Doe III*, 500 F. Supp. 2d at 420.

42. USA PATRIOT Improvement and Reauthorization Act § 106(f)(2), 120 Stat. at 198 (codified as amended at 50 U.S.C.A. § 1861(f)(2)(C)(ii) (West Supp. 2008)).

43. *Doe III*, 500 F. Supp. 2d at 411-16. *See* discussion *infra* pp. 475-78.

44. NSL Reform Act of 2007, S. 2088, 110th Cong. (as introduced in Senate, Sept. 25, 2007), attempts to address this issue by adding provisions allowing federal district courts *and* FISA courts to hear petitions.

45. USA PATRIOT Improvement and Reauthorization Act §106(a)(2), 120 Stat. at 196 (codified at 15 U.S.C.A. § 1861(a)(3) (West Supp. 2008)).

46. SECTION 215 AUDIT REPORT, *supra* note 17, at 9. But in a University of Illinois study in 2002, at least 3.1 percent of the responding librarians reported that they had received court orders prohibiting them from telling patrons that authorities requested information, and 2.6 percent of the librarians indicated that they did not answer some of the questions about service of an order because they believed they were legally prohibited

also added more congressional oversight of section 215 orders and increased the reporting requirements.[47] Before the Reauthorization Acts, the total number of section 215 orders that requested library or bookstore records had been the subject of highly contested litigation.[48]

III. LITIGATING SECTION 215—THE PUBLIC'S RIGHT TO KNOW HOW THE USA PATRIOT ACT HAS BEEN UTILIZED

Section 215 litigation has primarily involved Freedom of Information Act ("FOIA") requests.[49] *ACLU v. United States Department of Justice* ("*ACLU I*")[50] and *ACLU v. United States*

---

from doing so. LIBRARY RESEARCH CTR., UNIV. OF ILL. GRADUATE SCH. OF LIBRARY & INFO. SCI., PUBLIC LIBRARIES' RESPONSE TO THE EVENTS OF 9/11/2001: ONE YEAR LATER (2002) [hereinafter LIBRARIES' RESPONSE], http://lrc.lis.uiuc.edu/web/PLCLnum.pdf. There were 553 libraries that responded to the survey when it was initially sent out. Leigh S. Estabrook, *The Response of Public Libraries to the Events of September 11, 2001*, 84 ILL. LIBR. 1 (2002), http://www.cyberdriveillinois.com/publications/pdf_publications/illibrary_v84_n1.pdf. In conversations I have had with lawyers, most have assumed the librarians were "just mistaken." Of course, the librarians can't defend themselves. The request could have been informal, but referenced section 215; or, the library could have been the recipient of a letter stating that information should be preserved because a section 215 order was going to be issued. There is no way to know. But one thing the section 215 audit report illustrates is that the DOJ is extremely wary of anything to do with librarians.

47. USA PATRIOT Improvement and Reauthorization Act §106(h)(2), 120 Stat. at 199 (codified at 50 U.S.C.A. § 1862(b)(3) (West Supp. 2008)).

48. There have been six cases so far—four reported and two unreported—that have addressed section 215 since the passage of the USA PATRIOT Act. For the four reported cases, see ACLU v. U.S. Dep't of Justice (*ACLU I*), 265 F. Supp. 2d 20 (D.D.C. 2003); *ACLU II*, 321 F. Supp. 2d 24 (D.D.C. 2004); Elec. Privacy Info. Ctr. v. Dep't of Def., 355 F. Supp. 2d 98 (D.D.C. 2004) (deciding that plaintiff's request for expedited FOIA processing was denied, given the lack of evidence of any current public interest in data-mining software for antiterrorism programs, as opposed to general subject of "data mining"); Muslim Cmty. Ass'n of Ann Arbor v. Ashcroft, 459 F. Supp. 2d 592 (E.D. Mich. 2006) (holding that Muslim groups challenge of the constitutionality of section 215, alleging that it chilled their First Amendment rights, survived the government's standing challenge, but after the Reauthorization Acts amended section 215, the ACLU withdrew the complaint). For the unreported cases, see ACLU v. U.S. Dep't of Justice, No. C 04-4447 PJH, 2005 U.S. Dist. LEXIS 3763; 2005 WL 588354 (N.D. Cal. Mar. 11, 2005) (deciding that an ACLU FOIA request need not be processed on an expedited basis); Gerstein v. Cent. Intelligence Agency, No. C-06-4643 MMC, 2006 U.S. Dist. LEXIS 89883; 2006 WL 3462658 (N.D. Cal. Nov. 29, 2006) (deciding that a request for expedited FOIA processing of documents relating to unauthorized disclosure of classified documents was denied).

49. *See* cases cited *supra* note 48. The exception is *Muslim Community Ass'n of Ann Arbor v. Ashcroft*, which was a direct First Amendment challenge to section 215.

50. *ACLU I*, 265 F. Supp. 2d 20.

Department of Justice ("*ACLU II*")[51] are the cases that directly address the public's right to know about the government's use of section 215.[52] In *ACLU I*, the ACLU filed suit to compel the Department of Justice ("DOJ") to respond to a FOIA request for "aggregate statistical information revealing how often DOJ had used the Act's new surveillance and search provisions: roving surveillance under section 206; pen registers/trap-and-trace devices under section 214; demands for production of tangible things under section 215; and sneak and peek warrants under section 213."[53] The public debate about the effect of the USA PATRIOT Act on Americans' civil liberties was in full swing, and the ACLU was concerned that the DOJ had "provided only limited information to the public regarding how, and how often, the new provisions described above [had] been used."[54]

Some information about aggregate statistics had been released to Congress in a classified form,[55] and some was released only after congressional threats.[56] *ACLU I* was heard in the D.C. Circuit, which is notoriously deferential to claims of national security.[57] And this case was no different. The court deferred to the government's claims that releasing aggregate statistical information would somehow harm the national security, noting that Congress had authorized the release of aggregate statistical data to the public in only one category (orders approving electronic surveillance), but had limited the dissemination of other aggregate statistical information.[58] The court rejected the ACLU's argument which claimed that the mere publication of aggregate statistical

51. *ACLU II*, 321 F. Supp. 2d 24.

52. *ACLU I*, 265 F. Supp. 2d 20; *ACLU II*, 321 F. Supp. 2d 24.

53. *ACLU I*, 265 F. Supp. 2d at 25.

54. *Id.* at 24.

55. *Id.* at 24-25.

56. Congress' attempts to secure information about the implementation of the USA PATRIOT Act have been numerous and only partially successful. *See* PATRICK LEAHY, CHARLES GRASSLEY & ARLEN SPECTER, FBI OVERSIGHT IN THE 107TH CONGRESS BY THE SENATE JUDICIARY COMMITTEE: FISA IMPLEMENTATION FAILURES 9-10 (2003) [hereinafter LEAHY REPORT], www.fas.org/irp/congress/2003_rpt/fisa.pdf. Some answers were provided only after a threat to subpoena the Attorney General. Audrey Hudson, *Ashcroft Threatened with Hill Subpoena*, WASH. TIMES, Aug. 21, 2002, at A04. The LEAHY REPORT concluded: "The Congress and the *American people deserve to know what their government is doing.*" LEAHY REPORT, *supra*, at 14 (emphasis added).

57. *See* Nathan Slegers, Comment, *De Novo Review Under The Freedom Of Information Act: The Case Against Judicial Deference To Agency Decisions To Withhold Information*, 43 SAN DIEGO L. REV. 209, 212-13 (2006).

58. *ACLU I*, 265 F. Supp. 2d at 30-31.

information could not in and of itself harm national security, because if it did, then Congress would not have authorized release for any type of USA PATRIOT Act surveillance information.[59] The court also rejected the ACLU's argument that Congress was trying to get this aggregate information to the American people.[60] However, the Attorney General then voluntarily declassified the number of times the government had used section 215:

> This memorandum confirms I have declassified the number of times to date the [DOJ], including the [FBI], has utilized [s]ection 215 of the USA PATRIOT Act relating to the production of business records. The number of times [s]ection 215 has been used to date is zero (0).
>
> . . . .
>
> While Congress has regularly been informed regarding the number of times [s]ection 215 has been used, and while individual Members of Congress have been able to review that information, to date we have not been able to counter the troubling amount of public distortion and misinformation in connection with [s]ection 215. Consequently, I have determined that it is in the public interest and the best interest of law enforcement to declassify this information.[61]

The ACLU filed *ACLU II* after a new FOIA request, one for the number of times requests for section 215 orders had been submitted by field offices for approval and for other records relating to section 215, was denied.[62] The ACLU argued that the number of applications could have no bearing on national security unless they were approved, but the court once again deferred to the government's declaration that "the release of the number of section 215 field office requests poses the continuing potential to 'harm our national security by enabling our adversaries to conduct their intelligence or international terrorist activities more securely.'"[63] The court found that the number of applications would reveal the level of FBI activity, which might "also

59. *Id.*

60. *Id.* at 25; *see also* LEAHY REPORT, *supra* note 56, at 5, 13.

61. Memorandum from the Attorney Gen. to Dir. Robert S. Mueller (Sept. 18, 2003), http://www.cdt.org/security/usapatriot/030918doj.shtml.

62. *ACLU II*, 321 F. Supp. 2d 24, 27 (D.D.C. 2004).

63. *Id.* at 36.

permit an adversary to 'assess the exposure of business records to current or future operations' and to conclude that 'it is comparatively safe to conduct certain operations and activities based on the FBI's allocation and direction of resources.'"[64] However, as the court in *Gerstein v. United States Department of Justice*[65] pointed out, claiming that the release of statistical information about past practices would create a "road map" for future efforts aimed at purportedly disclosed weaknesses is "dubious" logic, as past practices are "hardly a reliable indicator that [the government] will continue [those practices]."[66]

IV. SECTION 215 AUDIT REPORT FINDS LITTLE UTILITY IN THIS FORM OF LEGAL PROCESS

Congress sided with the ACLU on the issue of making more information about the use of section 215 available to the public. Congress had been requesting similar information from the DOJ unsuccessfully, and the Reauthorization Act I includes an attempt to redress the problem. Every year, the Attorney General must submit an unclassified report to Congress containing, in addition to "the total number of applications made for [section 215 production] orders . . . and total number of such orders either granted, modified, or denied,"[67]

> the number of such [215] orders either granted, modified, or denied for the production of each of the following:
> (A) Library circulation records, library patron lists, book sales records, or book customer lists.
> (B) Firearms sales records.
> (C) Tax return records.
> (D) Educational records.
> (E) Medical records containing information that would identify a person . . . .[68]

---

64. *Id.* at 37.

65. Gerstein v. U.S. Dep't of Justice, No. C-03-04893 RMW, 2005 U.S. Dist. LEXIS 41276 (N.D. Cal. Sept. 30, 2005).

66. *Id.* at *40-*41 (denying plaintiff's request for FOIA records for summary statistics on the use of section 213 on other grounds).

67. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(h)(3), 120 Stat. 192, 200 (2006) (codified at 50 U.S.C.A. § 1862(c)(1)(A)-(B) (West Supp. 2008)).

68. *Id.* § 106(h)(2), 120 Stat. at 200 (codified at 50 U.S.C.A. § 1862(b)(3) (West

This third provision is new, and allows Congress and the public to have access to information about the use of section 215 in areas relating to privacy and other First Amendment rights.[69] In addition, the Reauthorization Act I requires the OIG of the DOJ to conduct a comprehensive audit of DOJ procedures, to review the effectiveness of section 215 authority, and report any abuses.[70] That audit was released in March of 2007.[71] The audit confirmed that section 215 had not been used before 2004: a "pure" section 215 order[72] was not approved until May of 2004, and a "combination" section 215 order was first approved in February of 2005.[73] There had been a total of twenty-one applications for pure section 215 orders from 2002 to 2005, but the first approval was in 2004.[74] No combination applications were even sent in until 2005.[75] The release of this information has had no apparent impact on national security, as none has been reported or alluded to by the government. The chart on the following pages summarizes the changes that were made to section 215 by the USA PATRIOT Act and the Reauthorization Acts.

Supp. 2008)).

69. *Id.* (codified at 50 U.S.C.A. § 1862(c)(2) (West Supp. 2008)).

70. *Id.* § 106A, 120 Stat. at 200.

71. *See* SECTION 215 AUDIT REPORT, *supra* note 17.

72. According to the Office of Intelligence Policy and Review ("OIPR"), a "pure" section 215 order is an "application for . . . tangible item[s] that is not associated with applications for any other FISA authority," while a "combination" application refers to a section 215 order that was added to a request for a FISA pen-register/trap-and-trace order. *Id.* at v-vi. For a copy of a section 215 order, see ACLU.org, http://www.aclu.org/patriot_foia/2003/215formorder.pdf.

73. SECTION 215 AUDIT REPORT, *supra* note 17, at 17, 35.

74. *Id.* at 17.

75. *Id.* at 35. *See id.* at 26-34 for a detailed discussion of the reasons section 215 orders were not approved.

	Before the USA PATRIOT Act	**After the USA PATRIOT Act**	**After the Re-Authorization Act**	**Proposed in the 110th Congress Issue**
Records	None allowed; section 215 orders limited to the records of "common carrier[s], public accommodation facilit[ies], physical storage facilit[ies], or vehicle rental facilit[ies]."[76]	"[A]ny tangible things (including books, records, papers, documents, and other items)" could be requested from any business or entity.[77]	The same, with an added "library provision": In the case of an application for an order for library circulation records or library patron lists, only three high-level employees are empowered to sign the application.[78] Records must be described with "sufficient particularity" to allow them to be identified.[79]	

76. 50 U.S.C. § 1862 (2000).
77. *Id.* § 1861 (Supp. II 2002).
78. 50 U.S.C.A. § 1861(a)(3) (West Supp. 2008).
79. *Id.* § 1861(c)(2)(A).

	Before the USA PATRIOT Act	**After the USA PATRIOT Act**	**After the Re-Authorization Act**	**Proposed in the 110th Congress Issue**
Standard to Issue	Although not applicable to library records, the standard was that "there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[80]	An application must state "that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[81]	Subsection (A) of 50 U.S.C. § 1861(b)(2) added the requirement that there be "*reasonable grounds to believe*" the records sought "*are relevant to an* authorized investigation," but that records are "*presumptively relevant*" if they pertain to three categories of agents of a foreign power or those in contact with such an agent.[82]	Section 9 of Senate Bill 2088 revises the standard to more closely conform to the pre-USA PATRIOT Act version (specific and articulable facts that the records pertain to a suspected agent of a foreign power or one in contact with an a suspected agent if there is a specifically identified national-security investigation).[83]

80. 50 U.S.C. § 1862(b)(2)(B) (2000).
81. *Id.* § 1861(b)(2) (Supp. II 2002).
82. 50 U.S.C.A. § 1861(b)(2)(A)-(A)(iii) (West Supp. 2008).
83. NSL Reform Act of 2007, S. 2088, 110th Cong. § 9 (2007).

	Before the USA PATRIOT Act	**After the USA PATRIOT Act**	**After the Re-Authorization Act**	**Proposed in the 110th Congress Issue**
Gag Order & Disclosure	Yes.	Yes. Left in place forever. Only disclose to those persons necessary for compliance with the production order. An attorney did not seem to be covered by this disclosure rule.[84] No specified penalty (contempt of court).	May disclose to "those persons to whom disclosure is necessary to comply with such order," and expressly permits the disclosure "to an attorney to obtain legal advice," as well as "other persons as permitted by the" FBI. Do not have to disclose the name of your attorney, but, if asked, must say who else knows of or will know of the order.[85] No specified penalty (contempt of court).	Section 9 of Senate Bill 2088 requires specific and articulable facts why the non-disclosure agreement is necessary and how it is narrowly tailored. Lasts 180 days unless extended.[86]

84. 50 U.S.C. § 1861(d) (Supp. II 2002).
85. 50 U.S.C.A. § 1861(d) (West Supp. 2008).
86. S. 2088 § 9.

	Before the USA PATRIOT Act	**After the USA PATRIOT Act**	**After the Re-Authorization Act**	**Proposed in the 110th Congress Issue**
Review of the Order	No.	No.	Yes, after one year, in the FISA court. 50 U.S.C. § 1861(f).[87] The judge may allow disclosure only if the original order to produce was "unlawful"; if the government certifies that there is a reason to believe "that disclosure may endanger the national security of the United States or interfere with diplomatic relations," the certification is conclusive and the recipient must wait another year to file amother request.[88]	Section 10 of Senate Bill 2088 allows review within twenty days in FISA court or district court.[89]
Sunset	No.	Yes, on 12/31/2005, but reauthorized.	Yes, on 12/31/2009.	N/A.

87. 50 U.S.C.A. § 1861(f) (West Supp. 2008).
88. *Id.*
89. S. 2088 § 10.

The section 215 audit not only lists the actual number of section 215 applications approved between 2000 and 2005—162 orders were approved and 31 applications were withdrawn—it discusses the reasons for withdrawals as well as the effectiveness of section 215 as an investigative tool.[90]

One of the orders prepared but never presented was an application for an order for library records.[91] The applicant's supervisor

> would not permit the request to go forward because of the political controversy surrounding [s]ection 215 requests for information from libraries. The [National Security Law Branch ("NSLB")] attorney who reviewed the request told the OIG that she attempted to get approval for the request but that her supervisor denied it because it involved a library. The Deputy General Counsel for NSLB told the OIG that he believed [the Office of Intelligence Policy and Review ("OIPR")] and the Department would disapprove of the FBI seeking information from a library, especially since the FBI had not yet obtained its first [s]ection 215 order.[92]

When the field office was advised that the application would not be sent, the field office obtained the information through other investigative means.[93] The report does not say which other investigative means were used.

The section 215 audit report found that the FBI was not very successful in obtaining section 215 orders: the various sections disagreed over legal interpretations, there were long delays in implementing policies and procedures, and there was insufficient funding to handle the requests.[94] And the OIG found that FBI agents did not understand the process for obtaining a section 215 order—agents just used other methods of getting the information, including NSLs, grand-jury subpoenas, and other process that was faster than a section 215

90. SECTION 215 AUDIT REPORT, *supra* note 17, at 17, 23, 26, 35, 73-74.

91. *Id.* at 28. The request for library records was submitted in November of 2003. *Id.* There was another order directed at a university library's records; that order was rescinded, apparently because of concerns about the Buckley Amendment. *Id.* at 31-32.

92. *Id.* at 28.

93. *Id.*

94. *Id.* at 60-63.

order.[95]

The section 215 audit report also found that "*the FBI did not create any analytical intelligence products based on the information obtained in response to pure* [*s*]*ection 215 orders*," and "*the evidence showed no instance where the information obtained from a* [*s*]*ection 215 order resulted in a major case development, such as the disruption of a terrorist plot.*"[96] The section 215 audit did note that the FBI began using section 215 more broadly in 2006, after the date of the section 215 audit.[97] But so far, an enormous amount of funding, personnel, and power has been transferred to the FBI with very little to show for it. The FBI did not articulate, and the section 215 audit report did not document, any real need for the expanded powers to secure business records that the USA PATRIOT Act conferred.

What the section 215 audit report did show was that political pressure by librarians was effective: no section 215 orders have been served on libraries.[98] But libraries and bookstores should be exempted from the whole process anyway. Section 215 orders are not as simple to secure as a search warrant, but are more constitutionally suspect: the rational compromise would be to subject library and bookstore records to legal process where there is the necessary nexus between the records and a specific crime, as the FBI appears to have done when the applicant could not secure a section 215 order for library records.

Although section 215 was scheduled to sunset in 2005, the

---

95. *Id.* at 63-64.

96. *Id.* at 79 (emphasis added). The orders were used primarily to exhaust investigative leads using information from "driver's license records; apartment leasing records; [and] credit card records." *Id.*

97. *Id.* at 80. In March, 2008, the second OIG audit was released. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006 (2008) [hereinafter SECTION 215 AUDIT REPORT II], http://www.usdoj.gov/oig/reports/FBI/index.htm. The SECTION 215 AUDIT REPORT II does not mention libraries at all, and does not revise any of the conclusions of the SECTION 215 AUDIT REPORT; it does mention, as a "noteworthy item," that after having an application turned down twice by the FISA court because "the facts were too 'thin' and . . . this request implicate[s] the target's First Amendment rights," the FBI issued NSLs for the very same information, despite an identical First Amendment limitation in the NSL statute. *Id.* at 33-34, 68. The FBI counsel stated "that she believed that it was appropriate to issue [the] NSLs because she disagreed with the FISA court." *Id.* at 72.

98. SECTION 215 AUDIT REPORT, *supra* note 17, at 80. One author has postulated that framing the debate in terms of *library records* and not *Internet records* had an adverse effect on the extent of the changes actually made in the Reauthorizations Acts. Andrew E. Nieland, Note, *National Security Letters and the Amended Patriot Act*, 92 CORNELL L. REV. 1201, 1227 (2007).

Reauthorization Act extended that sunset until December of 2009.[99] The section 215 audit report findings concerning the high cost, legal confusion, and limited utility of this program are good indications that the library community should continue to advocate for a return to pre-USA PATRIOT Act standards when this section comes up for review.

V. THE UPSTART CONTENDER—NATIONAL-SECURITY LETTERS

If the FBI has not been using section 215 to get library records, what has the FBI been using? Contrary to John Ashcroft's assertion that the FBI is not interested in what people are reading,[100] we know that libraries' computer records have been the subject of USA PATRIOT Act process, and that libraries have been asked for, and have provided, library records.[101] Since section 215 orders were so difficult to obtain, NSLs provided an easy alternative for some kinds of information.[102] An NSL is issued administratively by the agency—it is not issued by a court.[103] So the FBI can issue an NSL without any judicial oversight. NSLs have been around for a long time, and were originally drafted as limited exceptions to various statutes requiring stringent notice and hearing procedures.[104]

The form of NSL that concerns libraries allows the government to request subscriber information or electronic-communication transactional

99. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 102(b), 120 Stat. 192, 195 (2006) (codified at 50 U.S.C.A. § 1801 note (West Supp. 2008) (Sunset Provisions)).

100. "[T]he 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." Ashcroft, *supra* note 5.

101. Sometimes the FBI just asked for library records, and was given the information voluntarily. In a 2002 survey, 49.7 percent of the libraries responding voluntarily complied with informal law-enforcement requests for information about patrons' reading habits and Internet preferences in the previous year. LIBRARIES' RESPONSE, *supra* note 46. *See also* Dan Mihalopoulos, *Suit Contests Anti-Terror Patriot Act*, CHI. TRIB., July 31, 2003, at 10 ("An FBI official said Wednesday that Patriot Act powers have been employed about [fifty] times to examine library computer records. The official also said law-enforcement agents have not used the act to find out what books or other materials were checked out of libraries.").

102. *See* SECTION 215 AUDIT REPORT II, *supra* note 97, at 55-56.

103. 18 U.S.C. § 2709 (2000), *invalidated by Doe III*, 500 F. Supp. 2d 379 (S.D.N.Y. 2007).

104. For a general discussion of the evolution of NSLs, see generally Nieland, *supra* note 98, at 1206-11.

records from an "electronic communication service."[105] Libraries providing Internet and email access, either through an Internet web page or through a university email server, are included in the statutory definition of an "electronic communication service," and are required to comply with an NSL: "'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications . . . ."[106]

Despite this statutory language, NSLs were not the main focus for critics of USA PATRIOT Act process in the library, perhaps because of the seeming anonymity of much library computer use: many library computers have programs that automatically erase user history after a set amount of time.[107] However, when an anonymous internet service provider ("ISP") was served with an NSL in 2004 and filed suit to protest the non-disclosure provisions,[108] the debate about NSLs heated up. The attention of the library community became even more firmly engaged when a Connecticut library consortium was served with an NSL and filed suit to enjoin the non-disclosure provision so the recipients could engage in the public debate over the reauthorization of the USA PATRIOT Act.[109] Although the consortium director told the FBI that no particular Internet Protocol ("IP") address could be associated with any particular library or user months after the fact, the FBI agent assured the director that "we have our ways."[110]

---

105. USA PATRIOT Act, Pub. L. No. 107-56, § 505(a), 115 Stat. 272, 365 (codified at 18 U.S.C. § 2709(b) (Supp. I 2001)), *invalidated by Doe III*, 500 F. Supp. 2d 379. Section 2709(a) creates an exception to the statutory requirement that government agencies must get stored electronic communication information

> through compulsory process, such as a subpoena, warrant, or court order. *Section 2709 is a notable exception to these privacy protections because it permits the FBI to request records upon a mere self-certification—issued to the ISP or telephone company, not to the subscriber or to any court—that its request complies with the statutory requirements.*

Doe v. Ashcroft (*Doe I*), 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).

106. 18 U.S.C. § 2510(15) (2000).

107. George Christian, Executive Dir., Library Connection, Inc., They Rose to the Challenge: Public Librarians Take on the USA PATRIOT Act Through *Doe v. Gonzales*, Remarks at the American Association of Law Libraries Annual Meeting (July 14, 2007). The author's library has such a program on its public computers.

108. *Doe I*, 334 F. Supp. 2d 471. *See* discussion *infra* pp. 457-59.

109. Doe v. Gonzales (*Doe II*), 386 F. Supp. 2d 66 (D. Conn. 2005). *See* discussion *infra* pp. 457-59.

110. Christian, *supra* note 107. The consortium understood the FBI's request to mean

NSLs may be issued to request "subscriber information and toll billing records information, or electronic communication transactional records."[111] Before the USA PATRIOT Act, NSLs required the government to show "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."[112] That standard was lessened by the USA PATRIOT Act: the government need only certify that the records "are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the [F]irst [A]mendment to the Constitution of the United States."[113]

The types of records that can be requested on the government's self-certification of relevancy are actually fairly broad, because the statutory language is ambiguous. In its opinion on rehearing *Doe I*, the court stated

> [t]hat ambiguity is compounded because the NSL directs the recipient to determine for itself whether any information it maintains regarding the target of the NSL "may be considered . . . to be an electronic communication transaction record" in accordance with § 2709, but not "contents" of communications within the meaning of 18 U.S.C. § 2510(8). Such information might include the "to," "from," "date," and "time" fields of all emails sent or received, activity logs indicating dates and times that the target accessed the internet, the contents of queries made to search engines, and histories of

---

that *all* records from the relevant time period were being requested. *Id.* For a copy of the NSL served on the Connecticut library consortium, see ACLU.org, http://www.aclu.org/images/nationalsecurityletters/asset_upload_file924_25995.pdf.

111. 18 U.S.C. § 2709(a) (2000), *invalidated by Doe III*, 500 F. Supp. 2d 379 (S.D.N.Y. 2007). This section was not revised by the Reauthorization Acts.

112. *Id.* § 2709(b)(1)(B), *invalidated by Doe III*, 500 F. Supp. 2d 379.

113. USA PATRIOT Act, Pub. L. No. 107-56, § 505(a)(2)(B), 115 Stat. 272, 365 (codified at 18 U.S.C. § 2709(b)(1) (Supp. I 2001)), *invalidated by Doe III*, 500 F. Supp. 2d 379. And the USA PATRIOT Act expanded FBI issuing authority beyond FBI headquarter officials to include the heads of the FBI field offices. *Id.* § 505(a)(1) (codified at 18 U.S.C. § 2709(b) (Supp. I 2001), *invalidated by Doe III*, 500 F. Supp. 2d 379. NSLs always had a gag order, and there never has been a sunset provision for NSLs. *See* 18 U.S.C. §2709(c) (2000), *invalidated by Doe III*, 500 F. Supp. 2d 379. A United States person is a United States citizen, "an alien lawfully admitted for permanent residence," or certain associations or corporations. 50 U.S.C. § 1801(i) (2000).

> websites visited. Information requested by NSLs issued pursuant to § 2709 can also reveal the identity of an internet user associated with a certain email address, [IP] address, or screen name.[114]

The self-certification provisions of section 2709, and the lack of judicial review, meant that the FBI was the sole player in the process—the FBI decided who would be the target of an NSL, whether the request was "in the course of an authorized investigation," whether or not the recipient is a non-U.S. person or a U.S. person, and whether the investigation fully or partially implicated First Amendment activities.[115] No other branch of the government reviews this part of the process.[116]

VI. THE PRE-REAUTHORIZATION ACT CASES—*DOE I* AND *DOE II*

There has already been a fair amount written about the first two cases to challenge an NSL, but a brief review is necessary to set the stage for the debate about the Reauthorization Acts and the changes that were made to the NSL provisions.[117] *Doe I* was filed by a still-unknown ISP, alleging that the NSL statute violated the First, Fourth, and Fifth Amendments to the Constitution.[118] The district court found that the NSL statute prohibited the recipient from consulting an attorney,[119] was coercive to the reasonable recipient,[120] imposed a permanent prior restraint on speech in violation of the First Amendment,[121] and improperly precluded judicial review.[122] While the Fourth Amendment does not preclude issuing administrative subpoenas, there are Fourth

114. *Doe III*, 500 F. Supp. 2d at 387 (citation omitted).

115. *See* 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 121-24 (2007) [hereinafter NSL AUDIT REPORT], http://www.usdoj.gov/oig/special/s0703b/final.pdf.

116. This lack of review has been a focus of criticism of NSLs. *See* discussion *infra* pp. 473-74.

117. *See, e.g.*, Karl T. Gruben, *What Is Johnny Doing in the Library? Libraries, the U.S.A. PATRIOT Act, and Its Amendments*, 19 ST. THOMAS L. REV. 297 (2006); Nieland, *supra* note 98, at 1215-24.

118. *Doe I*, 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).

119. *Id.* at 496.

120. *Id.* at 503-04.

121. *Id.* at 512.

122. *Id.* at 506.

Amendment requirements that must be met for administrative subpoenas to pass constitutional muster, and the availability of a neutral tribunal to review the subpoena after it is issued is one of those requirements.[123] The NSL statute lacked the constitutional requirement that there be a neutral tribunal to determine, after a subpoena is issued, whether the subpoena actually complies with the Fourth Amendment's demands, and the district court held that the NSL provisions violated the Fourth Amendment as applied.[124] The court enjoined the government from enforcing the NSL provisions, but stayed the injunction to allow the government to appeal.[125]

The plaintiff in *Doe I* particularly wanted to be able to discuss, without revealing whose records had been requested or the nature of the information requested, the mere fact that the NSL had been served, the hardships the gag order had created in the recipient's personal and business life, and, most importantly, the plaintiff wanted to partake in the national discussion about NSLs that was taking place during the period when Congress was debating the Reauthorization Acts.[126] The court in *Doe I* had this to say about the scope of the gag order in section 2709:

> [T]he NSL statutes, unlike other legislation cited above, impose 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. . . . *This feature of § 2709(c) is extraordinary in that the breadth and lasting effects of its reach are uniquely exceptional, potentially compelling secrecy even under some decidedly non-sensitive conditions or where secrecy may no longer be justifiable under articulable national security needs.*[127]

The government appealed and the gag order remained in effect during the national debate on reauthorizing the USA PATRIOT Act; the government was successful in stifling dissent.[128] The anonymous

123. *Id.* at 495-96.
124. *Id.* at 526-27.
125. *Id.*
126. *My National Security Letter Gag Order*, WASH. POST, Mar. 23, 2007, at A17 [hereinafter *Gag Order*].
127. *Doe I*, 334 F. Supp. 2d at 519 (second emphasis added).
128. *See Gag Order*, *supra* note 126.

recipient has yet to be freed from the provisions of the gag order, despite the fact that the government no longer has any need for the information requested in the original order.[129]

In the second lawsuit to challenge NSLs, a Connecticut library consortium[130] that had been served with an NSL filed suit to lift the gag order so that it could participate in the national debate about the USA PATRIOT Act.[131] The district court's decision enjoined the government from enforcing the non-disclosure provision of section 2709(c) to the extent that the provision prevented the recipient from revealing its identity as a recipient of an NSL, holding that section 2709(c) did not satisfy the requisite First Amendment strict-scrutiny test, as it was not narrowly tailored to serve a compelling state interest.[132] Again, the injunction was stayed to allow the government to appeal.[133]

Although the identity of the plaintiffs in *Doe II* had been revealed in poorly redacted pleadings filed by the government, and publicized in the press,[134] the plaintiffs in *Doe II* were still governed by the gag order while the government appealed the district court order; they were similarly prevented from participating in the public debate about NSLs that had been taking place during the hearings on the Reauthorization Acts.[135]

George Christian is one of the Connecticut librarians who was served with an NSL in *Doe II*, and his was one of the voices that was silenced during the public debate. Mr. Christian spoke at the 2007 American Association of Law Libraries annual meeting. In both his presentation and his testimony before Congress in April of 2007, Mr. Christian was

129. *See Doe III*, 500 F. Supp. 2d 379, 387 n.3 (S.D.N.Y. 2007). The government dropped its request for the information in November of 2006. *See Gag Order*, *supra* note 126.

130. The consortium's "primary function is to provide a common computer system that controls the catalog information, patron records, and circulation information of our libraries. . . . At the time we were served with a national security letter, in July 2005, we were also providing telecommunications services to half our member libraries." *Hearing*, *supra* note 38, at 27 (statement of George Christian, Executive Director, American Library Association).

131. *Doe II*, 386 F. Supp. 2d 66 (D. Conn. 2005). At the time the consortium was served, the decision in *Doe I* had been issued.

132. *Id.* at 82.

133. *Id.* at 82-83.

134. Alison Leigh Cowan, *A Court Fight to Keep a Secret That's Long Been Revealed*, N.Y. TIMES, Nov. 18, 2005, at B1.

135. *See* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006). This is the opinion on the consolidated appeals in *Doe I* and *Doe II*.

eloquent about the need for libraries to continue their measured and thoughtful resistance to government fishing expeditions for library records.[136] The NSL he was served was not for material the FBI needed urgently—the NSL was not even delivered until almost two months after it was written.[137] The request was incredibly broad: in order for the FBI to "mine" for the information it requested, the consortium would have been required to turn over all records of computer use for all the computers in the library for the relevant time period.[138] The consortium needed the FBI's permission to even consult with an attorney.[139] And the government refused to allow any discussion of even the fact that an order had been served until after the Reauthorization Acts had passed.[140] The lengths to which the government was willing to go to prevent the consortium members from speaking out were striking. During court arguments in the Second Circuit on lifting the gag order, when the entire world already knew who the plaintiffs were,

> the government argued that merely revealing [the plaintiffs] as recipients of [an NSL] would violate national security. [The plaintiffs'] attorneys filed more legal papers to try to lift the gag, and attached copies of the New York Times articles. The government claimed that all the press coverage revealing [the plaintiffs'] names did not matter because 1) no one in Connecticut reads the New York Times and 2) surveys prove that 58% of the public disbelieves what they read in newspapers. To add to the absurdity, the government insisted that the copies of the news stories [the plaintiffs'] attorneys had submitted remain under seal in court papers. Even though [the plaintiffs'] names were not thoroughly redacted from the court documents, the government did redact from [the plaintiffs'] affidavits [their]

136. Christian, *supra* note 107; *Hearing*, *supra* note 38, at 27-35 (statement of George Christian, Executive Director, American Library Association). Mr. Christian is very clearly not a hothead, and seemed completely bewildered by the absurdity of the government's position on the need for secrecy. Among the passages in the pleadings that the government attempted to redact for national-security purposes, were portions of United States Supreme Court decisions. Christian, *supra* note 107.

137. Christian, *supra* note 107.

138. *Id.*

139. *See Hearing*, *supra* note 38, at 30 (statement of George Christian, Executive Director, American Library Association).

140. Doe v. Gonzales, 546 U.S. 1301 (2005) (declining to lift gag order). The gag order was not lifted until May 2006. *Gonzales*, 449 F.3d at 421.

> claim that forty-eight states had laws protecting the privacy of patron library records. [The plaintiffs] could not understand the threat to national security this information posed, but [they] did note that Attorney General Gonzales claimed to Congress that there was no statutory justification for claims of privacy.[141]

The government even tried to redact "direct quotes from Supreme Court opinions that undercut the government's arguments in the case."[142] One of the quotes was "The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent."[143]

After the Reauthorization Acts passed, the government withdrew its opposition to the disclosure of the identities of the *Doe II* recipients and then decided it did not need the information it had requested in the NSL; the Second Circuit dismissed *Doe II* as moot, and remanded *Doe I* to the district court in New York to determine the validity of the revised provisions of section 2709(c).[144] The government had successfully used the specter of national security to prevent dissent and stifle free speech, not to protect the public from terrorism.

VII. THE REAUTHORIZATION ACTS CHANGED THE USA PATRIOT ACT NSL PROVISIONS ON NONDISCLOSURE, JUDICIAL REVIEW, LIBRARIES, AND OVERSIGHT

The Reauthorization Act I amended the blanket prohibition on disclosure imposed by the USA PATRIOT Act.[145] A non-disclosure order will be included in an NSL only if a certification is added "that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or

141. Christian, *supra* note 107.

142. Press Release, ACLU, Reauthorized Patriot Act Still Unconstitutional, ACLU Says (Aug. 7, 2006), http://www.aclu.org/safefree/nationalsecurityletters/26404prs20060807.html.

143. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 314 (1972).

144. *Gonzales*, 449 F.3d at 421.

145. 18 U.S.C.A. § 2709(c) (West Supp. 2008), *invalidated by Doe III*, 500 F. Supp. 2d 379 (S.D.N.Y. 2007).

counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person."[146] While the gag order provision no longer automatically attaches to the NSL, it is still a self-certification process; no one reviews the need for certification. Given the FBI's position on disclosure in *Doe I* and *Doe II*, it is not surprising that the new guidelines for issuing NSLs indicate that "in most situations non-disclosure will be appropriate."[147] In 2006, under the new guidelines, at least ninety-seven percent of the NSLs examined imposed the non-disclosure requirements on recipients.[148]

If there is a non-disclosure certification, then the recipient may not disclose the NSL to anyone except those persons whose assistance is needed to comply with the order or to obtain legal advice; the recipient has to inform the FBI of the identity of those who have been, or will be told of the NSL, except that the recipient need not tell the FBI the attorney's identity.[149] So the right to consult with an attorney is now explicit. The recipient of an NSL also has to inform anyone who is told of the NSL of the non-disclosure requirements.[150] A specific penalty for violating the non-disclosure requirement has been added, and the penalty is severe:

> Whoever, having been notified of the applicable disclosure prohibitions or confidentiality requirements of section 2709(c)(1) of this title . . . knowingly and with the intent to obstruct an investigation or judicial proceeding violates such prohibitions or requirements applicable by law to such person *shall be imprisoned for not more than five years*, fined under this title, or

146. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 116(a), 120 Stat. 192, 213 (2006) (codified at 18 U.S.C.A. § 2709(c) (West Supp. 2008)), *invalidated by Doe III*, 500 F. Supp. 2d 379.

147. Memorandum from Gen. Counsel of Nat'l Sec. Law Policy & Training Unit to all FBI Divs. 12 (June 1, 2007), http://epic.org/privacy/nsl/New_NSL_Guidelines.pdf.

148. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBIS USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 160 (2008) [hereinafter NSL AUDIT REPORT II], http://www.usdoj.gov/oig/reports/FBI/index.htm.

149. USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, § 4(b), 120 Stat. 278, 280 (codified at 18 U.S.C.A. § 2709(c)(4) (West Supp. 2008)), *invalidated by Doe III*, 500 F. Supp. 2d 379.

150. USA PATRIOT Improvement and Reauthorization Act § 116(a), 120 Stat. at 213 (codified at 18 U.S.C.A. § 2709(c)(3) (West Supp. 2008)), *invalidated by Doe III*, 500 F. Supp. 2d 379.

both.[151]

VIII. JUDICIAL REVIEW

The Reauthorization Act I added a provision for judicial review of the scope of an NSL, by allowing the recipient to file a petition in federal district court for an order to modify or set aside the NSL.[152] In addition, the government was given the means to enforce an NSL by requesting a court order to compel compliance.[153] All proceedings regarding NSLs are closed.[154] A recipient may also a file petition to modify or set aside the non-disclosure requirement.[155] If the petition is filed within one year of the issuance of the NSL, the court can modify the non-disclosure requirement

> if it finds there is *no reason* to believe that *disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.* If, at the time of the petition, . . . [the government] certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such *certification shall be treated as conclusive unless the court finds that the certification was made in bad faith.*[156]

The "enumerated harms"[157] cover a lot of potential situations that have nothing to do with national security or terrorism, including *every* criminal investigation, and *any* threat of physical harm to a person.

---

151. *Id.* § 117, 120 Stat. at 217 (codified at 18 U.S.C.A. § 1510(e) (West Supp. 2008)) (emphasis added). The fine is $250,000 for an individual and $500,000 for an entity. 18 U.S.C. § 3571 (2000).

152. USA PATRIOT Improvement and Reauthorization Act §115, 120 Stat. at 211-13 (codified at 18 U.S.C.A. § 3511 (West Supp. 2008)), *invalidated in part by Doe III*, 500 F. Supp. 2d 379.

153. *Id.* (codified at 18 U.S.C.A. § 3511(c) (West Supp. 2008)).

154. *Id.* (codified at 18 U.S.C.A. § 3511(d) (West Supp. 2008)).

155. *Id.* (codified at 18 U.S.C.A. § 3511(b) (West Supp. 2008)), *invalidated by Doe III*, 500 F. Supp. 2d 379.

156. *Id.* (codified at 18 U.S.C.A. § 3511(b)(2) (West Supp. 2008)), *invalidated by Doe III*, 500 F. Supp. 2d 379 (emphasis added).

157. *Doe III*, 500 F. Supp. 2d at 389 (referring collectively to the conditions in the statute as the "enumerated harms").

If the petition to modify the non-disclosure requirement is made more than a year after the NSL was issued, then, within ninety days, a high-ranking official must either terminate the gag order or *recertify that lifting the gag order will endanger national security, "interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations," or endanger the life or safety of any person*; the government's recertification is conclusive unless it is made in bad faith.[158] If the government recertifies, the recipient of the gag order has to wait another year to request termination of the order.[159]

The reasons to get and maintain a gag order are broad, and include criminal investigations, so there is no need for a national security nexus to allow the government to prevent a recipient from speaking. And the government's certifications are conclusive, making judicial review illusory.

IX. THE LIBRARY EXEMPTION

The USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 ("Reauthorization Act II") added a "library" exemption: libraries that provide Internet access are exempt unless they are "providing the services defined in [18 U.S.C. §] 2510(15)."[160] However, since section 2510(15) defines an "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications,"[161] the exception may be so broad that it swallows the exemption. During the reauthorization debates, Senator Leahy stated that "[A] library may be served with an NSL only if it functions as a true [ISP], as by providing services to persons located outside the premises of the library. I expect that this will occur rarely or never and that in most if not all cases, the [g]overnment will need a court order to seize library records for foreign intelligence purposes."[162] John Conyers disagreed, stating that the exemption was nothing but a "fig

158. USA PATRIOT Improvement and Reauthorization Act § 115, 120 Stat. at 212 (codified at 18 U.S.C.A. § 3511(b)(3) (West Supp. 2008)), *invalidated by Doe III*, 500 F. Supp. 2d 379 (emphasis added).

159. *Id.*

160. USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, § 5, 120 Stat. 278, 281 (codified at 18 U.S.C.A. § 2709(f) (West Supp. 2008)), *invalidated by Doe III*, 500 F. Supp. 2d 379.

161. 18 U.S.C. § 2510(15) (2000).

162. 152 CONG. REC. S1558 (daily ed. Mar. 1, 2006) (Statement of Sen. Leahy).

leaf."[163] And apparently Robert Mueller, the director of the FBI, "in a written response to a Senate Judiciary Committee inquiry, even stated that new language 'did not actually change the law.'"[164]

Since many libraries are part of entities that do offer "electronic services" in the form of e-mail servers, or offer database or email services to patrons "outside the premises," these libraries—academic, law firm, library consortia, and public—would not be exempt even under a restrictive interpretation of the library exemption. While the scope of the exemption remains to be fully litigated, one lawsuit that has settled suggests the FBI thinks that libraries are not exempt; in *Internet Archive v. Mukasey*,[165] the FBI issued an NSL to the Internet Archive,[166] a digital library. The ACLU and the Electronic Frontier Foundation represented the Internet Archive, and were not only successful in convincing the FBI to withdraw the NSL, but also to lift the gag order, so that the service of the NSL on a library could be publicized.[167]

163. *Id.* at H585 (daily ed. Mar. 7, 2006) (Statement of Rep. Conyers).

164. *Hearing*, *supra* note 38, at 29 (statement of George Christian, Executive Director, American Library Association).

165. Internet Archive v. Mukasey, No. 07-6346-CW (N.D. Cal. 2008).

166. To view the Internet Archive website, see Internet Archive, http://www.archive.org (last visited Oct. 27, 2008).

167. Press Release, Elec. Frontier Found., FBI Withdraws Unconstitutional National Security Letter After ACLU and EFF Challenge: Gag Order Lifted on Internet Archive, Allowing Founder to Speak Out for First Time (May 7, 2008), http://www.eff.org/press/archives/2008/05/06.

The chart below summarizes the changes made to NSLs by the USA PATRIOT Act and the Reauthorization Acts.

18 U.S.C. § 2709	**Before the USA PATRIOT Act**	**After the USA PATRIOT Act**	**After the Re-Authorization Act**	**Proposals in the 110th Congress**
Records	Subscriber information, toll billing records, electronic communications transactional records.[168] By its terms, the statute covers identified customer's name, address, length of service, and billing information.[169]	The same.	The same.	House Bill 3189 prohibits letters containing unreasonable requirements or requiring privileged material.[170]

168. 18 U.S.C. § 2709(a) (2000), *invalidated by Doe III*, 500 F. Supp. 2d 379 (S.D.N.Y. 2007).

169. *Id.* § 2709, *invalidated by Doe III*, 500 F. Supp. 2d 379.

170. National Security Letters Reform Act of 2007, H.R. 3189, 110th Cong. § 3(c)(1) (2007).

18 U.S.C. § 2709	Before the USA PATRIOT Act	After the USA PATRIOT Act	After the Re-Authorization Act	Proposals in the 110th Congress
Standard to Issue	Specific and articulable facts that the information pertains to foreign power or its agent.[171]	Requires a certification of relevance and has the First Amendment prohibition.[172] You can ask for records for someone who is not the subject of the investigation .	The same.	House Bill 1739 adds the "specific and articulable facts" standard.[173] Senate Bill 2088 allows an NSL where there is an ongoing and authorized security investigation, *and* returns to the specific facts standard.[174] House Bill 3189 also requires a specific facts standard.[175]

171. 18 U.S.C. § 2709(b)(1)(B) (2000), *invalidated by Doe III*, 500 F. Supp. 2d 379.
172. *Id.* § 2709(b)(1) (Supp. I 2001), *invalidated by Doe III*, 500 F. Supp. 2d 379.
173. National Security Letter Judicial and Congressional Oversight Act, H.R. 1739, 110th Cong. § 2(a)(1) (2007).
174. NSL Reform Act of 2007, S. 2088, 110th Cong. § 2 (2007).
175. H.R. 3189 § 3(a)-(b).

18 U.S.C. § 2709	Before the USA PATRIOT Act	After the USA PATRIOT Act	After the Re-Authorization Act	Proposals in the 110th Congress
Gag Order & Disclosure	Yes[176] (no specific penalty/ contempt of court).	Yes (no specific penalty/ contempt of court).	Yes.[177] Penalty under 18 U.S.C. § 1510(e) of up to five years and fine of $25,000 for an individual and $500,000 for an organization;[178] may consult attorney.[179]	House Bill 1739 would make an Attorney General certification that disclosure will endanger the national security or interfere with diplomatic relations a rebuttable presumption, not a conclusive finding.[180] House Bill 3189 limits disclosure gag to thirty days.[181]

176. 18 U.S.C. § 2709(c) (2000), *invalidated by Doe III*, 500 F. Supp. 2d 379.

177. 18 U.S.C.A. § 2709(c) (West Supp. 2008), *invalidated by Doe III*, 500 F. Supp. 2d 379.

178. *Id.* § 1510(e) (2000).

179. *Id.* § 2709(c) (West Supp. 2008), *invalidated by Doe III*, 500 F. Supp. 2d 379.

180. National Security Letter Judicial and Congressional Oversight Act, H.R. 1739, 110th Cong. §2(b) (2007).

181. National Security Letters Reform Act of 2007, H.R. 3189, 110th Cong. § 3(d) (2007).

18 U.S.C. § 2709	Before the USA PATRIOT Act	After the USA PATRIOT Act	After the Re-Authorization Act	Proposals in the 110th Congress
Review of the Order	No.	No.	Yes.[182] Judicial review in federal court.[183]	House Bill 3189 authorizes judicial review for to modify or revoke a letter and adds ability to suppress evidence and file civil action for misuse of letters.[184] Senate Bill 2088 revises criteria for judicial review of non-disclosure orders.[185]

182. 18 U.S.C.A. § 3511 (West Supp. 2008), *invalidated in part by Doe III*, 500 F. Supp. 2d 379.

183. *See* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006).

184. H.R. 3189.

185. NSL Reform Act of 2007, S. 2088, 110th Cong. (2007).

18 U.S.C. § 2709	Before the USA PATRIOT Act	After the USA PATRIOT Act	After the Re-Authorization Act	Proposals in the 110th Congress
Library Section	No.	No.	Yes. Exempts libraries unless they provide the services listed in 18 U.S.C. § 2510(15);[186] exception is so broad it appears to swallow the exemption.	Libraries that host Internet services[187] are clearly not exempt under this section. Legislative history does not resolve the issue.
Sunset	N/A.	N/A.	N/A.	After five years, House Bill 3189 would require a reversion to law as it existed on October 25, 2001.[188] Senate Bill 2088 would terminate come authority for issuing NSLs on December 31, 2009.[189]

X. THE NSL AUDIT REPORT

The Reauthorization Acts expand congressional oversight of NSLs[190]

186. 18 U.S.C. § 2709(f) (West Supp. 2008), *invalidated by Doe III*, 500 F. Supp. 2d 379.
187. *See id.* § 2510(15) (2000).
188. H.R. 3189 § 5(a).
189. S. 2088 § 8.
190. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-

and call for an Inspector General's audit of the use of the authority.[191] In March of 2007, the Inspector General released its report concerning the use of NSLs for the years 2003 through 2005.[192] The NSL audit report is huge—the executive summary is over fifty pages—but there are many facts of interest to the library community and others concerned about the intersection of the First and Fourth Amendments.

The use of NSLs has increased dramatically, expanding from 8,500 requests in 2000 to 47,000 in 2005.[193] Because of poor or non-existent record keeping, the FBI's database "significantly understates the number of FBI NSL requests," but the total number listed as issued from 2003 through 2005 is 143,074.[194] Based on the NSL audit report's sample study of case files, the numbers in the database are underreported by seventeen percent.[195] Because of "delays in uploading NSL data and the flaws in the [Office of General Counsel ("OGC")][196] database, the total numbers of NSL requests that were reported to Congress semiannually in [calendar years] 2003, 2004, and 2005 were significantly understated."[197]

During the three years under review, the percentage of NSLs used to investigate "U.S. persons" increased from thirty-nine percent in 2003 to fifty-three percent in 2005.[198] The NSL audit report also found that in twelve percent of the case files examined, the investigative target of the NSL was described as a non-U.S. person when the target was described in the approval memoranda in the investigative file as, in fact, a U.S. person.[199] So in those cases, the FBI was able to ignore the First Amendment restrictions imposed on targeting U.S. persons.[200]

177, § 118, 120 Stat. 192, 217-18 (2006) (codified at 15 U.S.C. § 1681v(f) (2006)).

191. *Id.* § 119, 120 Stat. at 219-21. There was an additional 4.7% increase in the number of NSLs issued in 2006, to 49,425. NSL AUDIT REPORT II, *supra* note 148, at 159.

192. NSL AUDIT REPORT, *supra* note 115, at viii.

193. *Id.* at 120.

194. *Id.* at xviii.

195. *Id.* at xvi.

196. The OGC is the FBI's Office of General Counsel. *Id.* at xv.

197. *Id.* at xvii.

198. *Id.* at 38.

199. *Id.* at xlv-xlvi.

200. To issue the NSL, the FBI must self-certify that the records requested are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the [F]irst [A]mendment." 18 U.S.C. 2709(b)(2) (Supp. I 2001), *invalidated by Doe III*, 500 F. Supp. 2d 379 (S.D.N.Y. 2007).

The NSL audit report is critical of the FBI's initial performance: "[W]e found that . . . the FBI used NSLs in violation of applicable NSL statutes, Attorney General guidelines, and internal FBI policies."[201] And the NSL audit report found that the only FBI data-collection system produced "inaccurate" results,[202] and "a significant number of NSL-related possible violations are not being identified or reported" as required.[203] *Sixty percent* of the individual files examined "contained one or more violations of FBI internal control policies relating to [NSLs]."[204] The FBI regularly issued NSLs in a manner that provided no mechanism to ensure that NSLs were issued in the course of authorized investigations, or to ensure that the information sought in the NSLs was relevant to those investigations.[205] In other words, NSLs could be, and were, issued for records regardless of their nexus to national-security investigations.

The DOJ's own audit, a much larger sample than the NSL audit report, found similar numbers of misuses of orders, according to FBI General Counsel Valerie Caproni.[206] And the FBI's most recent review indicates that, in fact, "[t]he FBI improperly used [NSLs] in 2006 to obtain personal data on Americans during terror and spy investigations."[207] Despite the ease with which the agency could issue NSLs without substantive or procedural compliance with the law, there were times when the DOJ simply could not be bothered to meet its own minimal standards. For those situations, the agency used exigent letters.

---

201. NSL AUDIT REPORT, *supra* note 115, at 124.

202. *Id.* at 121.

203. *Id.* at 123. The NSL audit report found that twenty-two percent of the files reviewed contained unreported, NSL-related possible violations. *Id.*

204. *Id.*

205. *Id.*

206. John Solomon, *FBI Finds It Frequently Overstepped in Collecting Data*, WASH. POST, June 14, 2007, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/06/13/AR2007061302453.html ("'The FBI's comprehensive audit of [NSL] use across all field offices has confirmed the inspector general's findings that we had inadequate internal controls for use of an invaluable investigative tool,' FBI General Counsel Valerie E. Caproni said."). The audit covered ten percent of the records, and found potential violations of the law "or agency rules more than 1,000 times while collecting data about domestic phone calls, e-mails and financial transactions in recent years." *Id.*

207. Lara Jakes Jordan, *FBI Chief Says Report Will Show Additional Improper Use of Subpoenas in Terror, Spy Cases*, LAW.COM, Mar. 5, 2008, http://www.law.com/jsp/article.jsp?id=1204716628871. The report is a follow-up to the earlier report. *Id.*

XI. EXIGENT LETTERS

One of the problems the NSL audit report discussed was the use of exigent letters to get information before an NSL was issued.[208] Both in cases where there was no documented investigation and in cases where an NSL was never issued, exigent letters were issued at least *739 times*.[209] The letters typically stated: "Due to exigent circumstances, it is requested that records for the attached list of telephone numbers be provided. Subpoenas requesting this information have been submitted to the U.S. Attorney's Office who will process and serve them formally to [information redacted] as expeditiously as possible."[210]

The language of the letters could just as easily apply to providing an IP address as a telephone number. "[T]he 739 . . . letters requested information on [about] 3,000 different telephone numbers."[211] The service providers turned over records without ever receiving the NSL,[212] or turned over more information than the FBI requested.[213] A service provider who knowingly or intentionally violates the prohibition on providing "content" is subject to civil liability, but there are no criminal penalties for the breach.[214] If section 215 orders were too difficult for the FBI to use, NSLs turned out to be too easy.

The OIG—and librarians—are not the only groups to criticize the FBI for its misuse of NSLs. The Privacy and Civil Liberties Oversight Board (PCLO Board) was created by the Intelligence Reform and Terrorism Prevention Act of 2004.[215] One of the PCLO Board's statutory mandates is to "ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations, and *executive branch* policies related to efforts to protect the Nation against terrorism."[216] The PCLO Board's role is to advise and oversee. As part of its first statutory report, the PCLO Board said it

208. NSL AUDIT REPORT, *supra* note 115, at 86.
209. *Id.* at 86, 89.
210. *Id.* at 89.
211. *Id.* at 90.
212. *Id.*
213. Solomon, *supra* note 206.
214. 18 U.S.C. § 2707 (Supp. II 2002).
215. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1061, 118 Stat. 3638, 3684-88 (codified as amended at 42 U.S.C.A. § 2000ee (West Supp. 2008)).
216. *Id.* § 1061(c)(3), 118 Stat. at 3685 (codified as amended at 42 U.S.C. 2000ee(c) (West Supp. 2008)) (emphasis added).

would review the OIG report regarding the FBI's use of NSLs.[217] The PCLO Board is going to issue its own recommendations for solving the problems, but in the meantime, it had this to say: "The cause of protecting the nation from terrorism is not advanced by undermining the public's confidence in the government's ability to exercise investigative powers in compliance with applicable legal standards and required procedures. . . . Safeguards for privacy and civil liberties are not mere procedural formalities."[218]

The OIG agrees, and in its latest report to Congress, in which the goals for the DOJ are listed, the OIG

> added the challenge of "Restoring Confidence in the Department of Justice." The Department has faced significant criticism of its actions that has affected the morale of Department employees and the public confidence in the decisions of Department leaders. This turmoil, combined with numerous high-level vacancies, creates a significant challenge for Department leaders to reestablish public confidence in the independence and integrity of the Department.[219]

A goal carried over from previous reports was "to balance aggressive pursuit of its counterterrorism responsibilities with the need to protect individual privacy rights and civil liberties. This year, the OIG found significant problems in this challenge in an important area."[220] For the DOJ, "striking the appropriate balance between meeting its critical counterterrorism-related responsibilities and respecting civil rights, civil liberties, and privacy rights remains a key challenge."[221]

The FBI had not proved by specific examples that the current use of NSLs results in timely and useful intelligence. When the PCLO Board

---

217. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., FIRST ANNUAL REPORT TO CONGRESS: MARCH 2006-MARCH 2007 iii (2007). *A copy of the report is archived at http://blog.wired.com/27bstroke6/files/pclob_congress2007.pdf.*

218. *Id.* at iv.

219. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL SEMIANNUAL REPORT TO CONGRESS: APRIL 1, 2007-SEPTEMBER 30, 2007 39 (2007) [hereinafter SEMIANNUAL REPORT], *available at* http://www.usdoj.gov/oig/semiannual/0711/final.pdf.

220. Top Management and Performance Challenges in the Department of Justice-2007, http://www.usdoj.gov/oig/challenges/2007/index.htm#9 (last visited Oct. 1, 2008) [hereinafter Performance Challenges].

221. *Id.*

issued its second annual report, there was harsh criticism of the FBI's ability to defend the use of NSLs in their present form:

> [T]he FBI has not made a conscious, direct, and thorough effort to explain to the public and to Congress exactly why NSLs should be retained in their current form. Specifically, it has not made a comprehensive, detailed, and positive argument that NSLs collect essential information in the most timely and effective manner. It has not engaged critics of NSLs with sufficiently detailed information and specific instances of NSL use to allow policymakers to make informed decisions. It has also not described the elements of the current NSL regime that are essential to its operation. Finally, it has not discussed or shown how the current NSL regime appropriately limits risks to the privacy and civil liberties of U.S. Persons.[222]

While the challenges posed by the PCLO Board have still not been met, the second NSL audit report does finally include some actual examples of the utility of NSLs as an investigative tool—in eight cases out of 49,425 NSLs issued.[223]

XII. *DOE III*—THE NSL STATUTE STILL VIOLATES THE CONSTITUTION

Since some of the changes that were made to the NSL provisions directly addressed the constitutional deficiencies pointed out by the district court in *Doe I*, the case was remanded so that the plaintiff could amend its complaint in light of the Reauthorization Acts.[224] Judge Marrero ruled that the changes made by the Reauthorization Acts were insufficient to insulate NSLs from First Amendment and separation of powers challenges.[225] The *Doe III* court held that the revised non-disclosure provisions, which allowed the FBI to determine, on a case-by-case basis, whether a non-disclosure order should be included with the NSL, continued to act as a content-based restriction on speech by creating an impermissible licensing scheme in violation of the First

222. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., SECOND ANNUAL REPORT TO CONGRESS: MARCH 2007-JANUARY 2008 24 (2007), http://www.privacyboard.gov/reports/2008/congress2008.pdf.

223. NSL AUDIT REPORT II, *supra* note 148, at 114-16, 159.

224. *Doe III*, 500 F. Supp. 2d 379, 386 (S.D.N.Y. 2007).

225. *Id.* at 387.

Amendment.[226] The court noted:

> [u]nfortunately, one necessary consequence of the resulting discretion now afforded the FBI is that the amended 2709(c) creates the risk not only that an "entire topic" of public debate will be foreclosed, but also the risk that the FBI might engage in actual viewpoint discrimination. By now allowing the FBI to pick and choose which NSL recipients are prohibited from discussing the receipt of an NSL, conceivably the FBI can engage in viewpoint discrimination by deciding to certify nondisclosure when it believes the recipient may speak out against the use of the NSL and not to require nondisclosure when it believes the recipient will be cooperative.[227]

The district court also held that the standard prescribed by Congress for judicial review of the non-disclosure orders "is plainly at odds with First Amendment jurisprudence which requires that courts strictly construe content-based restrictions and prior restraints to ensure they are narrowly tailored to advance a compelling government interest."[228] The imposition of congressional standards of court review rendered judicial review illusory, and violated separation of powers.[229] The court held that "'Congress may not legislatively supersede our decisions interpreting and applying the Constitution,'"[230] and that such an attempt "breaches the proper constitutional limits drawn for our government by the concepts of separation and balance of power."[231]

One problem addressed by *Doe I* was not resolved by the Reauthorization Acts, and that is the problem that results when an NSL asks for transactional records without providing the recipient any guidance. The statute merely "directs the recipient to determine for itself

226. *Id.* at 425 ("[Section] 2709(c) is unconstitutional under the First Amendment because it functions as a licensing scheme that does not afford adequate procedural safeguards, and because it is not a sufficiently narrowly tailored restriction on protected speech.").

227. *Id.* at 397-98. In support of its opinion, the court also cited, as one of its authorities, the very Supreme Court quotation about the danger of acting under the vague concept of protecting domestic security that the FBI had originally redacted from the pleadings in *Doe II*. *See id.* at 407 (quoting *Keith*, 407 U.S. 297, 314 (1972)).

228. *Id.* at 409.

229. *Id.* at 411.

230. *Id.* (quoting Dickerson v. United States, 530 U.S. 428, 437 (2000)).

231. *Id.*

whether any information it maintains regarding the target of the NSL" is responsive, and whether the information is a "record" but not "contents."[232] So the response to an NSL could improperly reveal the "dates and times that the target accessed the [I]nternet, the contents of queries made to search engines, and histories of websites visited."[233] In fact, the second NSL audit report documents fourteen instances in 2006 where the recipient of the NSL provided too much information, including content, in response to an NSL.[234] In one of those instances, which was reported in the press, the FBI received the email messages from an entire computer network rather than one email subscriber; an anonymous intelligence official stated that "It's inevitable that these things will happen. It's not weekly, but it's common."[235]

Allowing the recipient of an NSL to determine what is "content," and then provide it to the government, means the government can acquire content without a warrant, which violates the Fourth Amendment requirement that a warrant be issued for content.[236] An NSL statute that allows the collection of content without a warrant is a statute in serious need of amendment. After both administrative and judicial investigation of NSL power, it is clear that the NSL statute gave the FBI and the executive branch too much discretion, which the FBI has been abusing. Giving one agency the power to determine the need for, issue, and

232. *Id.* at 387.

233. *Id.* The court's decision has, of course, been appealed. The appeal was filed November 6, 2007 in the Second Circuit (Docket No. 07-4943).

234. NSL AUDIT REPORT II, *supra* note 148, at 139-41.

235. Eric Lichtblau, *Through an Error, F.B.I. Gained Unauthorized Access to E-Mail*, N.Y. TIMES, Feb. 17, 2008, at A1.

236. The warrant requirement for process directed to content is a basic tenet of Fourth Amendment law. *Cf.* Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (discussing that no search had occurred and no warrant was required for a pen register which did not record content but only phone numbers dialed). Although the plaintiffs in *Doe I*, 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), dropped their Fourth Amendment due-process claims in light of the provision for judicial review added by the Reauthorization Acts, *Doe III*, 500 F. Supp. 2d at 389, other courts have held that vesting discretion in the recipient of an order to determine what is "content" in orders, such as pen-register orders, may violate the Fourth Amendment. *See, e.g.*, *In re* Application of the U.S. for an Order Authorizing Use of a Pen Register and Trap on (XXX) Internet Serv. Account/User Name (xxxxxxxx@xxx.com), 396 F. Supp. 2d 45, 49-50 (D. Mass. 2005) (denying the government's request for a pen-register order that might reveal content, such as search phrases in the URL, unless the order notified the recipient of the pen register specifically of what *could* be provided, and imposed contempt-of-court violations as a sanction for providing content). *See* discussion *infra* pp. 495-98 for a more comprehensive discussion of this and other pen register cases.

execute subpoenas without sufficient judicial oversight is not a model destined to produce restraint.[237]

The changes made to the NSL statute should not be permanent, and the debate over their use needs to continue. One of the three bills introduced in the 110th Congress to amend the NSL provisions has a sunset provision.[238] The National Security Letter Reform Act requires that section 2709 sunset in December of 2009, and that it revert to its pre-USA PATRIOT Act language.[239] This Bill would also limit the information that can be requested by an NSL, and limit the effect of the non-disclosure order to a narrowly tailored thirty-day order, renewable for one hundred eighty days.[240] Whether reforms take place in the 110th Congress or in the 111th Congress, they need to take place. It is too soon to stop pressuring Congress to revise the NSL statute.

XIII. USA PATRIOT ACT SEARCH WARRANTS

Search warrants have always been available to demand library records, computers, backup tapes, or any other tangible item.[241] Search warrants are immediately executable with or without the library's cooperation.[242] If a library is served with a search warrant, the normal procedure is to ask to see a copy, and make sure that nothing beyond

237. The FBI has been known to abuse its powers. In the 1970s, abuses of power led to the implementation of investigative guidelines, and the Senate committee set up to review the problem, the Church Committee, found that "[o]pposition to government policy or the expression of controversial views was frequently considered sufficient for collecting data on Americans." S. REP. NO. 94-755, at 169 (1976). The Church Committee worried that "[w]here unsupported determinations as to 'potential' behavior are the basis for surveillance of groups and individuals, no one is safe from the inquisitive eye of the intelligence agency." *Id.* at 177-78.

238. *See* NSL Reform Act of 2007, S. 2088, 110th Cong. § 8 (2007).

239. *Id.* §§ 2, 8. The two other bills about NSLs are the National Security Letter Judicial and Congressional Oversight Act, H.R. 1739, 110th Cong. (2007), which would require the approval of the FISC and would revise the deference a court should afford to the government's certification that disclosure would harm the national security to a rebuttable presumption, and the National Security Letters Reform Act of 2007, H.R. 3189, 110th Cong. (2007), which would limit the non-disclosure order to 180 days, would require specific facts in any government certification regarding the danger to national security, and would allow a motion to suppress evidence obtained unlawfully.

240. S. 2088 § 2.

241. "[A] search warrant may be directed to a library for any information, patron specific or [not]," so long as the material "has evidentiary value." Strickland, Minow & Lipinski, *supra* note 10, at 377.

242. *Id.* at 411.

what is specified in the warrant is searched or taken.[243] If a library is served with a search warrant—or other judicial process—cooperation and negotiation with law-enforcement officers is the best procedure to follow.[244] You can and should request a brief delay to consult with your counsel. The request might be granted or it might not, but you can always ask. This request was granted in *Tattered Cover, Inc. v. City of Thornton*, and the final result of granting that request for delay was the Colorado Supreme Court's decision, which refused to enforce the warrant for the bookstore's patron purchase records on both First and Fourth Amendment grounds.[245]

Polite but persistent refusal to comply with a request unless legal process is issued may also result in the demand disappearing, as happened to Washington librarian Joan Airoldi.[246] An FBI agent came into the library and *asked* for a list of all the people who had taken out a book on Osama bin Laden, and the library, after consultation with an attorney, refused.[247] The FBI then issued a subpoena[248] to try to find out who had written a quotation from a bin Laden speech in the margin of the book. The library trustees "voted unanimously to go to court to quash the FBI subpoena," and "[f]ifteen days later, the FBI withdrew its request."[249] But it was a bittersweet victory for Ms. Airoldi, who knew the result would have been different if her library has received a USA PATRIOT Act order:

> Fortunately for our patrons, we were able to mount a successful challenge to what seems to have been a fishing expedition. If it

243. *Id.* at 412.

244. *Id.* at 384.

245. Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Colo. 2002). The warrant was issued because the police found a mailer from the bookstore outside a meth lab, and two books on setting up drug labs; the police were trying to discover customer purchase records for the two books. *Id.* Long after the decision in the case, one of the defendants authorized the bookstore to release the information on the book that had been in the mailer: it was *A Guide to Remembering Japanese Characters* by Kenneth G. Henshall. David Grogan, *Reading Your Rights Tackles* Tattered Cover *Case*, AM. BOOKSELLERS ASS'N, Aug. 27, 2003, http://news.bookweb.org/freeexpression/1750.html.

246. Joan Airoldi, *Librarian's Brush With FBI Shapes Her View of the USA Patriot Act*, USA TODAY, June 17, 2005, http://www.usatoday.com/news/opinion/editorials/2005-05-17-librarian-edit_x.htm.

247. *Id.*

248. A subpoena is not issued by a court so it is not technically "legal process." *See* Strickland, Minow & Lipinski, *supra* note 10, at 379. It still cannot be ignored. *See id.*

249. Airoldi, *supra* note 246.

> had returned with an order from a secret court under the Patriot Act, the FBI might now know which residents in our part of Washington State had simply tried to learn more about bin Laden.
> With a Patriot Act order in hand, I would have been forbidden to disclose even the fact that I had received it and would not have been able to tell this story.[250]

When a library is served with a search warrant, and a request for court review prior to compliance is denied, the Fourth Amendment offers protection from the harshness of the warrant's service: a court has at least issued the warrant on a showing of probable cause;[251] after the warrant is served, the recipient can ask for a prompt determination of the legality of the warrant by a federal district court. If the warrant was improperly issued or implemented, the evidence seized pursuant to the warrant may be suppressed.[252] Also, there is a higher standard for search warrants that are issued for library records, as the warrant implicates

---

250. *Id.*

251. U.S. CONST. amend. IV; FED. R. CRIM. P. 41. Black's Law Dictionary defines probable cause as

> [a] reasonable ground to suspect that a person has committed or is committing a crime or that a place contains specific items connected with a crime. Under the Fourth Amendment, probable cause—which amounts to more than a bare suspicion but less than evidence that would justify a conviction—must be shown before . . . [a] search warrant may be issued.
>
> > Probable cause may not be established simply by showing that the officer who made the challenged arrest or search subjectively believed he had grounds for his action. . . . "If subjective good faith alone were the test, the protection of the Fourth Amendment would evaporate, and the people would be 'secure in their persons, houses, papers, and effects' only in the discretion of the police."

BLACK'S LAW DICTIONARY 1239 (8th ed. 2004) (quoting WAYNE R. LAFAVE & JEROLD H. ISRAEL, CRIMINAL PROCEDURE § 3.3, at 140 (2d ed. 1992)).

252. 3A WRIGHT, KING & KLEIN, *supra* note 11, § 677, at 400.

> If an unreasonable search has been made in violation of the Fourth Amendment, it is not merely the material seized that cannot be admitted in evidence. The government may not use the information thus improperly gained as a means of finding proper evidence. In what the Court has rightly called "a time-worn metaphor," the government is said to be barred from use of "a fruit of the poisonous tree."

Id. (footnotes omitted) (quoting Harrison v. United States, 392 U.S. 219, 222 (1968); Nardone v. United States, 308 U.S. 338, 341 (1939)).

First Amendment rights.[253]

The USA PATRIOT Act expanded the reach of search warrants by adding single-jurisdiction search warrants, which are good nationwide.[254] This allows a search warrant issued in one jurisdiction to be served in any jurisdiction, for an indefinite period of time. The USA PATRIOT Act also added delayed notice, or "sneak-and-peek" warrants, where the person whose records are being seized is not notified of the search until after the search has taken place.[255] Delayed notice warrants allow the government, "either physically or virtually," "to secretly enter a home or business," conduct the search, and leave without taking any "evidence or leaving notice of their presence."[256] The USA PATRIOT Act also broadened the types of electronic communications covered by search warrants.[257]

XIV. THE REAUTHORIZATION ACT I CHANGED THE NOTICE AND REPORTING REQUIREMENTS FOR SEARCH WARRANTS

The Reauthorization Act I changed the delayed-notification

253. Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978).

254. USA PATRIOT Act, Pub. L. No. 107-56, § 219, 115 Stat. 272, 291 (codified at FED. R. CRIM. P. 41 (Supp. I 2001)). Warrants may be issued "by a Federal magistrate judge in any district in which activities related to the terrorism may have occurred, for a search" anywhere in the country. *Id.* Pursuant to the USA PATRIOT Act, once the search warrant has been issued, it is valid nationwide. *Id.* § 220, 115 Stat. at 292 (codified at 18 U.S.C. § 2703 (Supp. I 2001)).

255. *Id.* § 213, 115 Stat. at 286 (codified at 18 U.S.C. § 3103a (Supp. I 2001)) (adding the "sneak-and-peak" provisions, which stated that any notice required by law to be given to the recipient of an order can be delayed "for a reasonable period," and the delayed notice can be extended "for good cause shown").

256. BRIAN T. YEH & CHARLES DOYLE, CONG. RESEARCH SERV., USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005: A LEGAL ANALYSIS 18 (2005), *available at* http://fas.org/sgp/crs/intel/RL33332.pdf.

257. USA PATRIOT Act § 209, 115 Stat. at 283 (codified at 18 U.S.C. §§ 2510, 2703 (Supp. I 2001)). Although the title of section 209 is "Seizure of Voice-Mail Messages Pursuant to Warrants," the actual changes in statutory language merely add the word "wire" to the statutes. *Id.* Several of the cases that have discussed search warrants as amended by the USA PATRIOT Act have focused on the whether the district where the crime is alleged to have occurred or the district where the records are held is the proper court to issue the warrant. The district where the alleged crime occurred (Arizona) was the proper district according to the court in *In re Search of Yahoo, Inc.*, No. 07-3194-MB, 2007 WL 1539971, at *7 (D. Ariz. May 21, 2007), although all the records were held by Yahoo in California. The court cited with approval the unpublished case *In Re Search Warrant*, No. 6:05-MC-168-Orl-31JGG, 2005 WL 3844032, at *13 (M.D. Fla. Dec. 23, 2005), agreeing that Congress intended "jurisdiction" to mean territorial jurisdiction.

requirements. Notice must now be given within thirty days of the date of the warrant, unless a request for an additional extension of time to give notice is granted.[258] Additional extensions of time to give notice are limited to periods of ninety days.[259] The Administrative Office of the Courts is now required to issue an annual report to Congress that includes the number of applications for delayed-notice search warrants, "and the number of such warrants and extensions granted or denied during the [previous] fiscal year."[260]

XV. DO THE DELAYED-NOTICE PROVISIONS MEET FOURTH AMENDMENT REQUIREMENTS?

Sneak-and-peek warrants allow surreptitious entry, and notice is not given until a "reasonable" period after the search.[261] In one case analyzing a USA PATRIOT Act delayed-notice search warrant, the district court thought that a *valid* delayed-notice search was probably constitutional, since "the Supreme Court has ruled 'the Fourth Amendment does not prohibit all surreptitious entries.'"[262] The district court also noted the limits on surreptitious entries:

> [T]he Ninth Circuit recognized: surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment demands that surreptitious entries be closely circumscribed.[263]

---

258. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 114, 120 Stat. 192, 210 (2006) (codified at 18 U.S.C.A. § 3103a(b)-(c) (West Supp. 2008)).

259. *Id.*

260. *Id.* § 114(c), 120 Stat. at 211 (codified at 18 U.S.C.A. § 3103a(d)(2) (West Supp. 2008)). The reporting requirement begins with the fiscal year ending September 30, 2007, so no report has yet been issued at the time of this writing. *Id.*

261. USA PATRIOT Act § 213, 115 Stat. at 286 (codified at 18 U.S.C. § 3103a (Supp. I 2001)).

262. United States v. Espinoza, No. CR-05-2075-7-EFS, 2005 WL 3542519, at *1 (E.D. Wash. Dec. 23, 2005) (quoting United States v. Frietas, 800 F.2d 1451, 1456 (9th Cir. 1986)).

263. *Id.*

Because the court that issued the delayed-notice search warrant had not made the required finding that there was "'reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result,'" and because the order did not specifically "'provide[] for the giving of such notice within a reasonable period of its execution,'" the court denied the government's motion to reconsider the order suppressing the evidence obtained with the improperly issued delayed-notice search warrant.[264]

XVI. SOME STATISTICS ON THE USE OF DELAYED-NOTICE SEARCH WARRANTS

There have been some statistics released on the use of delayed-notice search warrants. The DOJ released its initial data in 2003, revealing that during the period between October 26, 2001 and April 1, 2003, delayed-notice warrants had been used forty-seven times.[265] Requests for delayed-notice warrants doubled in the period between April of 2003 and January of 2005 to 108, for a total of 155 requests.[266] No request for delayed notice was ever denied.[267] "[A]pproximately [sixty] percent[]of [the] requests were granted under the broad justification that notice would have the result of 'seriously jeopardizing an investigation,' rather than under the more specific criteria that notice would endanger a person's life, imperil evidence, induce flight from prosecution or lead to witness tampering."[268] Some targets of delayed-notice search warrants have never been notified that they were the subjects of a clandestine search.[269] The chart on the following pages summarizes the changes made by the USA PATRIOT Act and Reauthorization Act I.

---

264. *Id.* at *2 (alteration in original) (quoting 18 U.S.C. §§ 3103a(b)(1), 3103a(b)(3) (Supp. I 2001)).

265. Press Release, Dep't of Justice, Department of Justice Releases New Numbers on Section 213 of the PATRIOT Act (Apr. 14, 2005), http://www.usdoj.gov/opa/pr/2005/April/05_opa_160.htm; *Implementation of the USA PATRIOT Act: Sections 201, 202, 223 of the Act That Address Criminal Wiretaps, and Section 213 of the Act that Addresses Delayed Notice: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 109th Cong. 28 (2005) (statement of Sen. Howard Coble, Chairman, Subcomm. on Crime, Terrorism, and Homeland Security).

266. *See* sources cited *supra* note 265.

267. *See* sources cited *supra* note 265.

268. *USA PATRIOT Act: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 6 (2005) [hereinafter *PATRIOT Act Hearing*] (statement of Bob Barr).

269. *See id.*

18 U.S.C. §§ 2510, 2703, 3103a; F.R. Crim.P. 41	**Before the USA PATRIOT Act**	**After the USA PATRIOT Act**	**After the Re-Authorization Act**	**Proposed Changes**
Records	Any tangible item with evidential value.	Expanded the kinds of electronic communications covered by search warrants.	The same.	
Standard to Issue, Scope & Notice	Probable cause to believe a person has committed or is committing a crime or that a place contains specific items connected with a crime. Contemporane-ous notice required in most cases.	The same certification, but with nation-wide, not district-wide, effect. Codification of ability to request delayed-notice search warrants. Delay in notice may be for a reasonable period of time.	Notice must be given within thirty days; request for extension up to ninety days.	Senate Bill 2435 would limit the authority to delay notice to seven days, and renewals to twenty-one days, and limits the causes for issuing a delayed notice by removing "unduly delaying a trial" from list of reasons might need delayed notice.[270]

270. Reasonable Notice and Search Act, S. 2435, 110th Cong. § 2 (2007).

18 U.S.C. §§ 2510, 2703, 3103a; F.R. Crim.P. 41	**Before the USA PATRIOT Act**	**After the USA PATRIOT Act**	**After the Re-Authorization Act**	**Proposed Changes**
Sunset	No.	No.	No.	Senate Bill 2435 would add this provision (section 213) to the list of USA PATRIOT Act sections that would sunset in December of 2009.[271]

The list of reasons why a delayed-notice warrant can issue includes several "catch-all" provisions. In addition to reasonable evidence of flight, destruction of evidence, intimidation of a witness, and danger to an individual, the court can issue a delayed-notice search warrant where there is serious jeopardy to an investigation, or undue trial delay.[272] Because of these "catch-all" provisions, the potential for abuse of delayed-notice search warrants cannot be ignored. Most delayed-notice search warrants could in fact be issued under the catch-all provisions.[273] A pending Senate bill addresses these problems by eliminating both serious jeopardy to an investigation and undue trial delay as reasons why a delayed-notice search warrant could issue, and requiring the delayed-notice provisions of the USA PATRIOT Act to expire.[274]

271. *Id.* § 3.
272. 18 U.S.C. § 2705(a)(2) (2000).
273. *PATRIOT Act Hearing*, *supra* note 268, at 49-50 (statement of James X. Dempsey, Executive Director, Center for Democracy and Technology).
274. S. 2435.

XVII. FISA WIRETAPS

A FISA roving wiretap is a general order that applies to any communication provider or ISP that a suspect uses; the order need not name the specific provider or ISP.[275] To have a request for a wiretap order from the FISC approved, the applicant must show that "there is *probable cause to believe that . . . the target . . . is a foreign power or an agent of a foreign power*"; the government does not have to show probable cause that one of the enumerated crimes has been or will be committed.[276] The government must also certify "that *a significant purpose of the surveillance is to [gather] foreign intelligence.*"[277] Prior to the passage of the USA PATRIOT Act, the government had to certify that *the* purpose of the surveillance was to gather foreign intelligence.[278] The USA PATRIOT Act also changed the scope of FISA wiretaps from district-wide to nationwide service, and the wiretap can be attached to any computer the target of the order uses, including a library computer.[279]

XVIII. SOME INTERPRETATIONS OF THE STATUTES

Only a few courts have directly addressed the constitutionality of the changes made by the USA PATRIOT Act to the FISA wiretap provisions. In one instance, a decision of the FISC denied the government's request to modify the existing minimization procedures for obtaining and sharing FISA electronic surveillance, holding that the government's proposed procedures gave criminal prosecutors too much power to direct and control FISA searches or surveillance.[280] This

275. *See* 50 U.S.C. § 1805 (2000).

276. 50 U.S.C. § 1805(a) (2000) (emphasis added).

277. 50 U.S.C. § 1804(a)(7)(B) (Supp. I 2001).

278. USA PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (codified at 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(b) (Supp. I 2001)).

279. *Id.* § 206, 115 Stat. at 282 (codified at 50 U.S.C. § 1805(c)(2)(B) (Supp. I 2001)).

280. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (FISA Ct. 2002), *abrogated by In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002). This excessive power destroyed the "wall" between domestic criminal investigations and foreign intelligence investigations in a manner that was not consistent with FISA's mandate "to 'obtain, produce, and disseminate foreign intelligence information.'" *Id.* at 623 (emphasis omitted) (quoting 50 U.S.C. §§ 1801(h), 1821(4) (2000)). Prior to the district court's decision, the government had violated the existing minimization procedures seventy-five times by erroneously alleging a FISA target was not under criminal investigation, omitting material facts about the relationship between

decision was overruled in the first—and only—published decision of the FISA Court of Review, *In re Sealed Case*,[281] which issued a decision on the scope of the "significant purpose" language.[282] The government's argument that it could use a FISA wiretap warrant if the *primary* purpose of the investigation was prosecuting an agent for a nonforeign intelligence crime was rejected, but the court approved authorizing a warrant where the government asserted *any measurable foreign intelligence purpose*.[283]

In *Mayfield v. United States*,[284] the government used the FISC's process without any really good evidence that the target was an agent of a foreign power.[285] In March of 2004, Brandon Mayfield was arrested as a suspect in the terrorist bombing in Madrid.[286] Mayfield is an American-born citizen, an army officer with an honorable discharge, a practicing lawyer, had never been arrested, and had not traveled out of the country since 1994; he is also a practicing Muslim.[287] Although the fingerprint-match evidence for one of Mayfield's fingerprints was questionable, the FBI sought and received broad search warrants for Mayfield's home and office; he was arrested and his family was told that he was being held as a primary suspect in the terrorist bombing in Madrid, and that there was a 100% match for his fingerprints.[288] These stories were leaked to the press.[289] Several weeks into Mayfield's detention, the Spanish authorities notified the government that they had matched the fingerprint to an Algerian, and Mayfield was released.[290] Mayfield filed suit, charging that the government's searches under FISA, which allowed for circumvention of the Fourth Amendment's probable

---

the FBI and a FISA target, and making erroneous statements about meeting the minimization procedures. *Id.* at 620-21.

281. *In re* Sealed Case, 310 F.3d 717.

282. *Id.*

283. *Id.* at 735-39. DOJ has interpreted this section to mean that FISA wiretaps can be used primarily for criminal-investigation purposes. *The USA PATRIOT Act in Practice: Shedding Light on the FISA Process: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. 20 (2002) (statement of William C. Banks, Professor of Law, Syracuse University).

284. Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007).

285. *Id.* at 1026-29.

286. *Id.* at 1029.

287. *Id.* at 1027.

288. *Id.* at 1029.

289. *Id.*

290. *Id.*

cause requirements, violated the Constitution.[291]

Mayfield's complaint directly attacked the "significant purpose" language added by the USA PATRIOT Act. He alleged that the government can improperly avoid the strictures of the Fourth Amendment "merely by asserting a desire to also gather foreign intelligence information from the person whom the government intends to criminally prosecute," so long as the government represents that the target was an agent of a foreign power.[292] The government's representation is an assertion the court must accept unless clearly erroneous.[293] The court agreed with Mayfield, stating:

> Now, for the first time in our Nation's history, the government can conduct surveillance to gather evidence for use in a criminal case without a traditional warrant, as long as it presents a non-reviewable assertion that it also has a significant interest in the targeted person for foreign intelligence purposes.[294]

The government relied on *In re Sealed Case*, but the court rejected the government's position that the case was "highly persuasive," disputing the reasoning of the case, and noting that even the *In re Sealed Case* court conceded that "'the constitutional question presented by this case—whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment—has no definitive jurisprudential answer.'"[295] The *Mayfield* court found the analysis in *In re Sealed Case* contradictory and unnecessary: the "wall" and any "dangerous confusion" the wall generated had been removed by another provision of the USA PATRIOT Act, and criminal investigators are free to seek Title III orders for criminal investigations, with that Title's definitions having been expanded to include "virtually all terrorism and espionage-related offenses."[296] The *Mayfield* court's final problem with the government's position was based on fundamental issues of the appropriate checks and balances required by the Constitution:

> Moreover, the constitutionally required interplay between

291. *Id.* at 1030.
292. *Id.* at 1032-33.
293. *Id.*
294. *Id.* at 1036.
295. *Id.* at 1041 (quoting *In re* Sealed Case, 310 F.3d 717, 743 (FISA Ct. Rev. 2002)).
296. *Id.*

> Executive action, Judicial decision, and Congressional enactment, has been eliminated by the FISA amendments. . . . The Constitution contains bedrock principles that the framers believed essential. Those principles should not be easily altered by the expediencies of the moment.
>
> Despite this, the FISCR holds that the Constitution need not control the conduct of criminal surveillance in the United States. In place of the Fourth Amendment, the people are expected to defer to the Executive Branch and its representation that it will authorize such surveillance only when appropriate. The defendant here is asking this court to, in essence, amend the Bill of Rights, by giving it an interpretation that would deprive it of any real meaning. This court declines to do so.
>
> For over 200 years, this Nation has adhered to the rule of law—with unparalleled success. A shift to a Nation based on extra-constitutional authority is prohibited, as well as ill-advised. . . .
>
> . . . I conclude that 50 U.S.C. §§ 1804 and 1823, as amended by the Patriot Act, are unconstitutional because they violate the Fourth Amendment of the United States Constitution.[297]

Several other cases have looked at the overlap between criminal and foreign-intelligence investigations in the context of requests to suppress the use of evidence obtained in a foreign-intelligence investigation in a trial for domestic crimes. These cases have focused on the differing standards for probable cause for a Title III warrant and a FISA warrant. These defendants have not been so successful. In *United States v. Ning Wen*,[298] the defendant was being tried for "violating the export-control laws by providing militarily useful technology to the People's Republic of China without the required license," based on evidence from a FISC order for international-terrorism surveillance.[299] The court found that there was no constitutional prohibition on using the evidence from a FISA order in a domestic crime case:

> Probable cause to believe that a foreign agent is communicating with his controllers outside our borders makes an interception

297. *Id.* at 1042-43.
298. United States v. Ning Wen, 477 F.3d 896 (7th Cir. 2007).
299. *Id.* at 897.

> reasonable. If, while conducting this surveillance, agents discover evidence of a domestic crime, they may use it to prosecute for that offense. That the agents may have known that they were likely to hear evidence of domestic crime does not make the interception less reasonable than if they were ignorant of this possibility.... It is enough that the intercept be adequately justified without regard to the possibility that evidence of domestic offenses will turn up. Interception of Wen's conversations was adequately justified under FISA's terms, so there is no constitutional obstacle to using evidence of any domestic crimes he committed.[300]

In *United States v. Damrah*,[301] the defendant "was found guilty of unlawfully obtaining citizenship ... by making false statements in a citizenship application and interview."[302] Some of the evidence was reviewed *ex parte* by the court, as it had been obtained pursuant to a FISC order; the court summarily rejected Damrah's Fourth Amendment claim.[303] And a FISA warrant was upheld in *United States v. Rosen*,[304] where the defendants were charged with conspiring to communicate national defense information; the defendants were U.S. persons whose lobbying activities were partly protected by the First Amendment. The court ruled that the government's allegations that some of the

300. *Id.* at 898-99.

301. United States v. Damrah, 412 F.3d 618 (6th Cir. 2005).

302. *Id.* at 620.

303. *Id.* at 624-25. The court noted that "FISA has uniformly been held to be consistent with the Fourth Amendment," citing *In re Sealed Case* with approval. *Id.* at 625. Of course *Mayfield* had not been decided yet. In several other cases, defendant's motions to suppress have been denied, sometimes on procedural grounds, as in *United States v. Jayyousi*, No. 04-60001-CR, 2007 WL 781373, at *1 (S.D. Fla. Mar. 12, 2007) (rejecting claims that defendant's actions were protected by the First Amendment). In *United States v. Benkahla*, 437 F. Supp. 2d 541 (E.D. Va. 2006), the court rejected the defendant's claim that his computer was illegally seized; the court only analyzed pre-USA PATRIOT Act case law as no other authority had been provided. *Id.* In *United States v. Holy Land Foundation for Relief and Development*, No. 3:04-CR-240-G, 2007 WL 2011319 (N.D. Tex. July 11, 2007), the defendants, charged with funding terrorist organizations such as Hamas, alleged that the primary purpose of the surveillance was criminal, but the district court relied on the analysis in *In re Sealed Case* that was rejected by the *Mayfield* court and held that FISA did not violate the Fourth Amendment. *Id.* at *5. In *United States v. Marzook*, 435 F. Supp. 2d 778, 780 (N.D. Ill. 2006), the court was faced with a pre-USA PATRIOT Act FISA warrant for a physical search, and held that the search was reasonable and was authorized for "foreign intelligence."

304. United States v. Rosen, 447 F. Supp. 2d 538 (E.D. Va. 2006).

defendants' lobbying activities were unlawful were sufficient to overcome the statutory bar on using FISA for activities protected by the First Amendment.[305]

The question of whether or not the commingling of criminal investigations with foreign intelligence investigations, as currently authorized by FISA, comports with the Fourth Amendment remains to be finally resolved. Faced with a clear case where the government used the FISC, and its simpler standards of probable cause, when it was pursuing a criminal claim, the *Mayfield* court found that FISA did not comport with the Fourth Amendment.[306] But where the facts differed in that the original aim of the investigation was to obtain foreign intelligence, and the defendant was later charged with a crime, the courts have been just as motivated to find that FISA does comport with the Fourth Amendment.

XIX. CHANGES MADE BY THE REAUTHORIZATION ACTS

In order to get a court order authorizing a wiretap, the crime must be statutorily designated a "predicate offense."[307] The Reauthorization Act I expanded the list of predicate offenses to include

> crimes relating to biological weapons, violence at international airports, nuclear and weapons of mass destruction threats, explosive materials, receiving terrorist military training, terrorist attacks against mass transit, arson within U.S. special maritime and territorial jurisdiction, torture, firearm attacks in federal facilities, killing federal employees, killing certain foreign officials, conspiracy to commit violence overseas, harboring terrorists, assault on a flight crew member with a dangerous weapon, certain weapons offenses aboard an aircraft, aggravated identity theft, "smurfing" (a money laundering technique whereby a large monetary transaction is separated into smaller transactions to evade federal reporting requirements on large transactions), and criminal violations of certain provisions of the Sherman Antitrust Act.[308]

305. *Id.* at 541, 548-49.
306. Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007).
307. 18 U.S.C. § 2516 (2000).
308. YEH & DOYLE, *supra* note 256, at 24.

The Reauthorization Act I added a requirement that the government describe the specific target of a wiretap in its application for an order when the target's identity is not known, and added a requirement that the government articulate specific facts in support of an application for a roving wiretap.[309] When the government changes the location of the roving surveillance to a new location that was not known at the time of the application, the court issuing the wiretap must be notified within ten days.[310] A description of the total number of applications for roving wiretaps made each year now has to be reported to congressional committees.[311] The Reauthorization Act I extends the expiration date of the section of the USA PATRIOT Act authorizing roving wiretaps to December 31, 2009.[312]

XX. SOME STATISTICS ON WIRETAPS

The Administrative Office of the United States Courts issues a yearly report on electronic surveillance in general, and in 2005, state and federal courts authorized 1,773 interceptions of wire, oral, and electronic communications, an increase over the previous year.[313] Only one application was denied by the courts.[314] In 2004, state and federal courts authorized 1,710 interceptions of wire, oral, and electronic communications.[315] This was an increase of nineteen percent over intercepts approved in 2003.[316] Federal officials applied for 730

309. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 108, 120 Stat. 192, 203 (2006) (codified at 50 U.S.C.A. §§ 1804(a)(3), 1805(c)(1)(A) (West Supp. 2008)).

310. *Id.* § 108(b)(4) (codified at 50 U.S.C.A. § 1805(c)(3) (West Supp. 2008)).

311. *Id.* § 108(c)(2), 120 Stat. at 204 (codified at 50 U.S.C.A. § 1808(a)(2) (West Supp. 2008)).

312. *Id.* § 102(b), 120 Stat. at 195 (codified at 50 U.S.C.A. § 1805 note (West Supp. 2008) (Sunset Provisions)).

313. LEONIDAS RALPH MECHAM, ADMIN. OFFICE OF THE U.S. COURTS, REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 5 (2006), *available at* http://epic.org/privacy/wiretap/2005_wiretap_report.pdf. The report does not include FISA orders.

314. *Id.*

315. LEONIDAS RALPH MECHAM, ADMIN. OFFICE OF THE U.S. COURTS, REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 5 (2005), *available at* http://www.uscourts.gov/wiretap04/2004WireTap.pdf.

316. *Id.*

intercept orders in 2004, a twenty-six percent increase over the number requested in 2003.[317] No wiretap applications were denied.[318] In 2003, there were 1,442 interceptions of wire, oral, and electronic communications, an increase of six percent over interceptions authorized in 2002.[319] The agency also reported that federal officials applied for 578 intercept orders in 2003, a sixteen percent increase over those requested in 2002.[320] No wiretap applications were denied.[321] These statistics do not include FISA roving wiretaps; information available on FISA roving wiretaps is included in a letter report the Attorney General makes to Congress, which showed that applications for FISA surveillance orders have also increased over the reported years, and that applications are not denied.[322] The chart on the following pages describes the changes made to the roving-wiretap laws by the USA PATRIOT Act and the Reauthorization Act I.

317. *Id.*

318. *Id.* at 7.

319. LEONIDAS RALPH MECHAM, ADMIN. OFFICE OF THE U.S. COURTS, REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 5 (2004), *available at* http://www.uscourts.gov/wiretap03/2003WireTap.pdf.

320. *Id.*

321. *Id.* at 7.

322. *See* Letter from William E. Moschella, Assistant Attorney Gen., U.S. Dep't of Justice, to Dennis Hastert, Speaker, U.S. House of Representatives (Apr. 28, 2006) [hereinafter Speaker Letter Two], http://www.fas.org/irp/agency/doj/fisa/2005rept.html; Letter from William E. Moschella, Assistant Attorney Gen., U.S. Dep't of Justice, to Dennis Hastert, Speaker, U.S. House of Representatives (Apr. 1, 2005) [hereinafter Speaker Letter One], http://www.fas.org/irp/agency/doj/fisa/2004rept.pdf. *See also infra* notes 342 and 343 and accompanying text.

50 U.S.C. §§ 1804, 1805	**Before the USA PATRIOT Act**	**After the USA PATRIOT Act**	**After the Re-Authorization Act**
Records	Electronic surveillance attaches to a telephone or a computer. Recovers content.	Suspect, not a particular telephone or computer; in some circumstances, the order does not have to identify the third parties who need to assist in implementing the wiretap.	
Standard to Issue	Probable cause that the "target of the electronic surveillance is a foreign power or an agent of a foreign power . . . . [N]o [U.S.] person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the [F]irst [A]mendment to the Constitution . . . ."[323]	The same certification, but with nation-wide, not district-wide, effect.	Applications for orders, as well as orders, have to identify the *specific* target of electronic surveillance or specifies the type of description if the target's identity is not known; new locations must be disclosed to the court within ten days.[324]

323. 50 U.S.C. § 1805(a)(3)(A) (2000).
324. *See* 50 U.S.C.A. § 1804 (West Supp. 2008); *Id.* § 1805.

50 U.S.C. §§ 1804, 1805	**Before the USA PATRIOT Act**	**After the USA PATRIOT Act**	**After the Re-Authorization Act**
Gag Order & Disclosure	Yes, must comply with order and "accomplish the electronic surveillance in such a manner as will protect its secrecy"[325] (no specific penalty/contempt of court).	The same.	The same.
Review of the Order	Implied, not specific.	The same.	The same.
Sunset	N/A	Yes.	December 31, 2009.[326]

XXI. SECTION 216 & SECTION 214 PEN REGISTER/TRAP-AND-TRACE ORDERS

The USA PATRIOT Act expanded the scope of pen register/trap-and-trace orders[327] in national-security cases. There are two types of pen

325. 50 U.S.C. § 1805(c)(2)(B) (2000).

326. 50 U.S.C.A. § 1805 note (West Supp. 2008) (Sunset Provisions).

327. "'A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released.'" Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979) (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977)). The trap-and-trace device is the reverse of a pen register; it records incoming information. 18 U.S.C. § 3127(4) (Supp. I 2001). Both will be referred to as "pen registers." Because recording incoming and outgoing telephone numbers was not considered a "search" requiring a warrant under *Smith v. Maryland*, 442 U.S. at 745-46, the original pen-register statute offered more procedural protection than had been available. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

register orders that were changed by the USA PATRIOT Act. Section 216 affected pen register orders issued by federal courts, and allowed the courts to issue pen register orders for real-time interception of non-content information from computers, not just from telephones.[328] Section 214 gave the FISC the same expanded authority.[329] It was section 216 orders that got all the press, but section 216 was unchanged by the Reauthorization Acts.

One of the issues left unresolved by the remorseless advance of technology has been how to deal with the fact that IP addresses and telephone numbers have the capability to reveal content. Even telephone calls can reveal a lot more content than the number dialed. When you call the bank and give your account information, or call the pharmacy and order prescriptions using a credit card on an automated system, you reveal content. When a device uses tone detection to generate a list of all digits dialed after a call has been connected, it "is called 'post-cut-through dialed digit extraction.'"[330] IP addresses also can reveal content. In *In re Application of U.S. for an Order Authorizing Use of a Pen Register & Trap On (XXX) Internet Serv. Account/User Name, (xxxxxxxx@xxx.com)*, the court was troubled by the government's application for

> [IP] addresses[,] which are defined as a "unique numerical address identifying each computer on the internet." The [ISP] would be required to turn over to the government the incoming and outgoing IP addresses "used to determine web-sites visited" using the particular account which is the subject of the pen register.
>
> . . . .

328. USA PATRIOT Act, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288-90 (codified at 18 U.S.C. §§ 3121, 3123, 3124, 3127 (Supp. I 2001)). For a more detailed discussion of the changes made to section 216 by the USA PATRIOT Act, see Susan Nevelow Mart, *Protecting the Lady From Toledo: Post-USA PATRIOT Act Electronic Surveillance at the Library*, 96 LAW LIBR. J. 449, 452-53 (2004).

329. USA PATRIOT Act § 214, 115 Stat. at 286-87 (codified at 50 U.S.C. §§ 1842-1843 (Supp. I 2001)).

330. *In re* Application of U.S. for an Order Authorizing Use of a Pen Register & Trap On (XXX) Internet Serv. Account/User Name, (xxxxxxxx@xxx.com), 396 F. Supp. 2d 45, 48 n.2 (D. Mass. 2005) (quoting U.S. Telecomm. Ass'n v. FCC, 227 F.3d 450, 456 (D.C. Cir. 2000)). *See also In re* Application of U.S. For an Order Authorizing the Installation and Use of a Pen Register and a Trap & Trace Device on E-Mail Account, 416 F. Supp. 2d 13 (D.D.C. 2006) (granting the government's request for a pen-register order for non-content email information).

> . . . A user may visit the Google site. Presumably the pen register would capture the IP address for that site. However, if the user then enters a search phrase, that search phrase would appear in the URL after the first forward slash. This would reveal content . . . .[331]

The court was concerned that ISPs would not be alert to the subtle distinctions between "incoming and outgoing IP addresses" and content, and rewrote the pen register order so that the ISP had to configure its software so that "*subject lines, application commands, search queries, requested file names, and file paths*" would not be recovered, and imposed possible contempt of court penalties on the ISP for failure to comply.[332] The court hoped that technology could solve the problem of improper collection of content. So far, courts have relied on government assertions that ISPs can remove content from the information provided.[333]

In the case of telephone numbers, technology is not currently up to the challenge. In a case from the Southern District of Texas, the court denied the government's application for a pen register order involving cell phones because the government had declared that "'technology currently is not reasonably available which would permit law enforcement to reliably discern and then separately collect only those post-cut-through digits that are call processing information from those that may constitute content.'"[334] The court rejected the government's pledge that it would make no affirmative use of content digits, and held that the USA PATRIOT Act amendments require more than over-collection of content and promises not to use it: "shall not include contents" is a clear statutory commandment, and the government either needs to develop better technology or use other statutory means to obtain the information.[335]

---

331. *In re Application of U.S. for an Order Authorizing Use of a Pen Register & Trap On (XXX) Internet Serv. Account/User Name, (xxxxxxx@xxx.com)*, 396 F. Supp. 2d at 48-49.

332. *Id.* at 49-50.

333. *See* cases cited *supra* note 330.

334. *In re* United States, 441 F. Supp. 2d 816, 822-23 (S.D. Tex. 2006). *See also In re* U.S. for Orders (1) Authorizing Use of Pen Registers and Trap & Trace Devices, 515 F. Supp. 2d 325 (E.D.N.Y. 2007); *In re* United States, No. H-07-613, 2007 WL 3036849, at *9 (S.D. Tex. 2007) (refusing to issue a pen-register order for post-cut-through dialed digits).

335. *In re United States*, 441 F. Supp. 2d at 825-26.

The Sixth Circuit has expressly ruled on the limits of collecting emails before the Fourth Amendment must be satisfied: to/from addresses and IP addresses are not content and can be recovered without a warrant, but URLs that reveal what page of a website a user viewed are content and a warrant based on probable cause must be issued before content can be recovered.[336] Section 214 pen register orders are issued by the FISC,[337] but otherwise the post-USA PATRIOT Act processes are similar. Both section 216 and section 214 orders could attach to a library computer, and if library equipment is not able to record what the government wants, the government can attach its own equipment.[338]

XXII. CHANGES MADE BY THE REAUTHORIZATION ACT I

The 2006 amendments changed several things about FISA pen register orders. The scope of information that can be provided pursuant to a pen register order was expanded by the Reauthorization Act I, and the court may now order the service provider to turn over customer information as well as the dialing or Internet address information.[339] The duration of the order may now be up to one year: if "the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a United States person, an order, or an

336. Warshak v. United States, 490 F.3d 455, 469-76 (6th Cir. 2007). This analysis was followed by the court in *In re U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 534 F. Supp. 2d 585 (W.D. Pa. 2008), to deny the government's request for cell-phone-subscriber information for use in identifying the user's past or present physical or geographical location.

337. USA PATRIOT Act, Pub. L. No. 107-56, § 214, 115 Stat. 272, 286-87 (codified at 50 U.S.C. §§ 1842-1843 (Supp. I 2001)).

338. *Id.* § 216(b)(1), 115 Stat. at 288-89 (codified at 18 U.S.C. § 3123 (Supp. I 2001)). The software developed by the government was known as Carnivore, and is now known as DCS 1000. *Confirmation Hearing on the Nomination of Robert S. Mueller, III to be Director of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. 108 (2001) (statement of Robert S. Mueller).

339. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 128, 120 Stat. 192, 229 (2006) (codified at 50 U.S.C.A. § 1842(d)(2)(C) (West Supp. 2008)). The information includes the name and address of the customer or subscriber; the telephone or instrument number, or other subscriber number or identifier of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information; how long the target has been a customer of the provider and the terms of service; if it is a telephone service, any local or long-distance telephone records of the customer or subscriber; any records reflecting period of usage (or sessions) by the customer or subscriber; and information about payment, including credit-card or bank-account numbers. *Id.*

extension of an order, under this section may be for a period not to exceed one year."[340] Reauthorization Act I also requires additional reporting: the Judiciary Committee must receive full reports on the use of pen registers/trap-and-trace devices every six months.[341]

XXIII. SOME STATISTICS ON THE USE OF FISA COURT PROCESS

The information that is available about the FISC is not very specific. In "2005, the [g]overnment made 2,074 applications to the . . . [FISC] for authority to conduct electronic surveillance and physical search for foreign intelligence purposes," of which 2,072 "applications for authority to conduct electronic surveillance and physical search" were approved.[342] In 2004, the government made 1,758 applications to the FISC for authority to conduct electronic surveillance and physical search for foreign-intelligence purposes, and none were denied.[343] The changes made to section 214 pen registers are summarized in the chart on the pages that follow.

340. *Id.* § 105, 120 Stat. at 195-96 (codified at 50 U.S.C.A. § 1842(e)(2) (West Supp. 2008)).

341. *Id.* §128(b), 120 Stat. at 229 (codified at 50 U.S.C.A. § 1846(a) (West Supp. 2008)).

342. Speaker Letter Two, *supra* note 322. "The FISC made substantive modifications to the [g]overnment's proposed orders in [sixty-one] of those applications." *Id.* "The FISC did not deny, in whole or in part, any application filed by the [g]overnment during calendar year 2005." *Id.*

343. Speaker Letter One, *supra* note 322.

50 U.S.C. § 1842	Before the USA PATRIOT Act	After the USA PATRIOT Act	After the Re-Authorization Act
Records and Duration	Telephone numbers dialed within a specific federal district.	Real-time interception of "non-content" information from computers, as well as telephones. All orders are roving orders, and are good for ninety days.	Initial orders for non-U.S. persons can be requested or renewed for as long as one year.[344] Courts may authorize release of customer information in addition to dialing or IP information.[345]
Standard to Issue	Certification to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.	The same certification, but with nation-wide, not district-wide, effect.	The same.
Gag Order & Disclosure	Yes, unless or until ordered by the court. Order lasts sixty days, with renewals (no specific penalty).	The same.	The same.
Review of the Order	Yes.	The same.	The same.
Library Section	No.	No.	No.
Sunset	N/A	No.	No.

344. 50 U.S.C.A. § 1842(e)(2) (West Supp. 2008).
345. *Id.* § 1842(d)(2)(C).

XXIV. FISHING EXPEDITIONS—WHAT IS ALL THIS IN AID OF?

Looking at government fishing expeditions for information, both more narrowly in the case of libraries and bookstores, which have traditionally been safe havens for access to information, or more broadly in the case of government data-mining efforts,[346] one must ask if the implementation of the USA PATRIOT Act has been a benefit to the cause of preventing terrorism. The balance between the preservation of civil liberties and the prevention of terrorism has always been the crux of the surveillance problem, whether you believe that the government has been overzealous in its efforts to prevent terrorism at the expense of civil liberties, or believe that it has not been zealous enough. So a brief look at the government's own analysis of what terrorist acts it has managed to prevent since it was granted expanded powers by the USA PATRIOT Act should be instructive.

The DOJ just published *Terrorism 2002-2005*,[347] to "provide[] an overview of the terrorist incidents and preventions designated by the FBI as having taken place in the United States and its territories during the years 2002 through 2005 and that are matters of public record."[348] From September 12, 2001 through 2005, the DOJ lists twenty-seven incidents of terrorist attacks in the United States.[349] Twenty-two of those incidents were perpetrated by the Earth Liberation Front or the Animal Liberation Front and involved crimes against property.[350] The remaining five incidents are as follows:

---

346. Although a discussion of all of the government's broad data-collection efforts is beyond the scope of this article, the government's efforts at fishing expeditions have not been limited to the library. For a review of the government's attempts to maintain broad databases of information on "U.S. persons," see for example Frederick M. Joyce & Andrew E. Bigart, *Liability For All, Privacy For None: The Conundrum of Protecting Privacy Rights in a Pervasively Electronic World*, 41 VAL. U. L. REV. 1481 (2007); Andrew P. MacArthur, Note, *The NSA Phone Call Database: The Problematic Acquisition and Mining of Call Records in the United States, Canada, the United Kingdom, and Australia*, 17 DUKE J. COMP. & INT'L L. 441 (2007); Steven W. Dummer, Comment, *Secure Flight and Data Veillance, a New Type of Civil Liberties Erosion: Stripping Your Rights When You Don't Even Know It*, 75 MISS. L.J. 583 (2006).

347. FED. BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, TERRORISM 2002-2005 (2006) [hereinafter TERRORISM], *available at* http://www.fbi.gov/publications/terror/terrorism2002_2005.pdf.

348. *Id.* at iii. The terrorism report also includes major FBI investigations overseas and identifies significant prosecutorial updates, legislative actions, and program developments relevant to counter-terrorism efforts.

349. *Id.* at 65-66.

350. *Id.*

- the 2001 Anthrax mailings with no known perpetrator (5 deaths);
- a shooting at Los Angeles International Airport by Hesham Mohamed Ali Hedayat (2 deaths);
- two separate bombings in California suspected to have been committed by Daniel Andreas San Diego, an animal-rights activist; and
- an arson in Oklahoma City attributed to Sean Michael Gillespie of the Aryan Nation.[351]

The terrorism report concluded that the longstanding trend is *that "domestic extremists [carry] out the majority of terrorist incidents" in the United States.*[352] Regarding terrorist preventions, defined as "a documented instance in which a violent act by a known or suspected terrorist group or individual with the means and a proven propensity for violence is successfully interdicted through investigative activity,"[353] the terrorism report has this to say:

> The terrorist preventions for 2002 through 2005 paint a more diverse threat picture. Eight of the [fourteen] recorded terrorist preventions stemmed from right-wing extremism, and included disruptions to plotting by individuals involved with the militia, white supremacist, constitutionalist and tax protester, and anti-abortion movements. The remaining preventions included disruptions to plotting by an anarchist in Bellingham, Washington, who sought to bomb a U.S. Coast Guard station; a plot to attack an Islamic center in Pinellas Park, Florida; and a plot by a prison-originated, Muslim convert group to attack U.S. military, Jewish, and Israeli targets in the greater Los Angeles area. In addition, *three preventions involved individuals who sought to provide material support to foreign terrorist organizations, including al-Qa'ida, for attacks within the United States.*[354]

351. *Id.*
352. *Id.* at 29 (emphasis added).
353. *Id.* at v.
354. *Id.* at 29 (emphasis added).

These three preventions took place in 2005, and involved a lone person's meeting with undercover officers to present a design for a bomb that the suspect "intended to build and sell"; the arrest of two armed robbers who were allegedly raising money for a Muslim convert organization founded in prison; and the arrest of one person at a motel in Pocatello, Idaho after he arranged "to meet a purported al-Qa'ida contact."[355]

So the apparatus of the war on terror has been directed at animal rights activists, homegrown right-wing types, two armed robbers, and two want-to-be terrorists who met with undercover officers. There is, of course, no way of knowing the extent to which the expanded powers granted to the government by the USA PATRIOT Act contributed to these preventions. Although we know that the use of section 215 orders has not contributed to a prevention,[356] other USA PATRIOT Act legal process may have contributed to these preventions, and prevention is a worthy goal.

But the DOJ has yet to meet its goal of "striking the appropriate balance between meeting its critical counterterrorism-related responsibilities and respecting civil rights, civil liberties, and privacy rights."[357] The USA PATRIOT Act needs to be revised to mandate criteria that impose that balance. It takes years for the orders of courts to become final and affect agency policy. It is not too much to ask of our representatives that they pass legislation that protect civil liberties because, as Thomas Jefferson pointed out, "In questions of power, then, let no more be heard of confidence in man, but bind him down from mischief by the chains of the Constitution."[358]

355. *Id.* at 25. *See also* Guy Lawson, *The Fear Factory*, ROLLING STONE, Feb. 7, 2008, at 60 (discussing a story on the Joint Terrorism Task Force and some overblown claims of terrorist cells). *Rolling Stone* also has an online list of all of the Bush Administration's terrorist alerts, the lack of factual intelligence information that might form a basis for the alert, and what else was happening in the news on any given day that was embarrassing to the administration. *See* Tim Dickinson, *Truth or Terrorism? The Real Story Behind Five Years of High Alerts: A History of the Bush Administration's Most Dubious Terror Scares and the Headlines They Buried*, ROLLING STONE, Feb. 7, 2008, http://www.rollingstone.com/politics/story/18056504/truth_or_terrorism_the_real_story_behind_five_years_of_high_alerts.

356. SECTION 215 AUDIT REPORT, *supra* note 17, at 79.

357. Performance Challenges, *supra* note 220.

358. Jefferson, *supra* note 1, at 161.