

University of California, Hastings College of Law

Faculty Services Librarian and Adjunct Professor of Law

March 2008

The Chains of the Constitution and Legal Process in the Library: a Post-Patriot Reauthorization Act Assessment

Contact
Author

Start Your Own
SelectedWorks

Notify Me
of New Work



Available at: http://works.bepress.com/susan_nevelow_mart/1

Abstract:

Since the Patriot Act was passed in 2001, controversy has raged over nearly every provision. The controversy has been particularly intense over provisions that affect the patrons of libraries. This article follows those Patriot Act provisions that affect libraries, and reviews how they have been interpreted, how the Patriot Reauthorization Acts have changed them, and what government audits and court affidavits reveal about the use and misuse of the Patriot Act. The efforts of librarians and others opposed to the Patriot Act have had an effect, both legislatively and judicially, in changing and challenging the Patriot Act. Because libraries are such a potent symbol of democratic openness, the effect of the Patriot Act on libraries has acted in the public mind as a microcosm of the broader problems with the implementation of the Patriot Act. The public's discomfort with the civil liberties implications of the Patriot Act has turned out to be justified, as every agency that has reviewed the implementation of the Patriot Act has concluded that the government has not been able to maintain an appropriate balance between the need to protect civil liberties and the need to prevent terrorist acts. The government's list of domestic terrorist acts that have been prevented or punished is not inspiring: the entire panoply of tools authorized by the Patriot Act has not done much more than stop some home-grown right wing fringe groups and ecoterrorists. In light of the evidence of abuse of civil liberties and the questionable constitutionality of many of the Patriot Act's provisions, this paper suggests that the time for vigorous advocacy has not passed and that further legislative changes need to be made.

Table of Contents

I. Introduction.

II.

Section 215 – The Library Provision.

Section 215 Was Substantially Changed by the Reauthorization Act.

Litigating Section 215 – the Public's Right to Know How the Patriot Act Has been Utilized.

Section 215 Audit Report Finds Little Utility in This Form of Legal Process.

Chart of Section 215 Changes.

III.

The Upstart Contender – National Security Letters.

The Pre-Reauthorization Act Cases – Doe I and Doe II.

The Reauthorization Acts Changed the Patriot Act NSL Provisions On Nondisclosure, Judicial Review, Libraries, and Oversight.

Judicial Review.

The Library Exemption.

Chart of NSL Changes.

The NSL Audit Report.

Exigent Letters.

Doe III: The NSL Statute Still Violates the Constitution.

IV.

Patriot Act Search Warrants.

Reauthorization Act I Changed the Notice and Reporting Requirements for Search Warrants.

Do the Delayed Notice Provisions Meet 4th Amendment Requirements?

Some Statistics on the Use of Delayed Notice Search Warrants.

Chart of Delayed Notice Search Warrant Changes.

V.

FISA Wiretaps.

Some Interpretation of the Statutes.

Changes Made by the Reauthorization Acts.

Some Statistics on Wiretaps.

Wiretap Chart.

VI.

Section 216 & Section 214 Pen Register/Trap & Trace Orders.

Changes Made by the Reauthorization Act I.

Some Statistics on the Use of FISA Court Process.

Chart of Section 214 Changes.

VII.

Fishing Expeditions – What is All This In Aid of?

The Chains of the Constitution and Legal Process in the Library: a Post-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. **

The forms of legal process¹ authorized by the Patriot Act,² as they apply to library patron information, implicate both First Amendment and Fourth Amendment values.³ Seizing evidence of what you're thinking about by looking at what you're reading or what you're 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 Patriot Act's incursions into this realm of intellectual

* 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, Jul. 17, 2007. © 2008 Susan Nevelow Mart

* 30 THE PAPERS OF THOMAS JEFFERSON 543-49 (2003).

¹ Legal process is a generic term for a court order to produce documents or information. BLACK'S LAW DICTIONARY 1242 (8th ed. 2004).

² Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [Patriot Act].

³ See *Tattered Cover, Inc. v. City of Thornton*, 44 P.2d 1044 (Colo. 2002).

freedom. And the government has heaped scorn on librarians for their opposition.⁴ 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 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,⁵ which sought the help of librarians in reporting "suspicious" readers of unclassified information, was the passage of state statutory protection for library records.⁶ Although the statutes vary widely in their

⁴ See, e.g., John Ashcroft, *Protecting Life and Liberty* (Sept. 18, 2003), <http://www.usdoj.gov/archive/ag/speeches/2003/091803memphisremarks.htm>; Eric Lichtblau, *At FBI, Frustration Over Limits on an Antiterror Law*, Dec. 11, 2005, NY TIMES, 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."

⁵ HERBERT N. FOERSTAL, *SURVEILLANCE IN THE STACKS: THE FBI'S LIBRARY AWARENESS PROGRAM*, 133-34 (1991).

⁶ *State Laws on the Confidentiality of Library Records*, http://www.library.cmu.edu/People/neuhaus/state_laws.html. All but two states have statutes expressly protecting library records; the two states without statutes (Kentucky and Hawai'i)

specificity, most do make an exception for libraries to provide records pursuant to a court order.⁷ The judicial review requirement for a court order 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.⁸ With most court issued orders, because a library is being asked to produce records,⁹ there is an opportunity to consult with an attorney before compliance.¹⁰ Libraries are not required to, and may violate state law, if they turn over

have opinions from their attorneys general that library records are confidential. MARY MINOW & TOMAS A. LIPINSKY, *THE LIBRARY’S LEGAL ANSWER BOOK* 200–10 (2003).

⁷ *Id.*

⁸ Where the government seeks to discover library records because the *content* of what a patron has read or viewed is at issue, the First Amendment requires the strictest scrutiny before any legal process can issue. *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1059 (Colo. 2002): “...the chilling effect that results from disclosure of customer purchase records 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.”

⁹ Lee S. Strickland, Mary Minow, Thomas Lipinski, *A Patriot in the Library: Management Approaches When Demands for Information Are Received From Law Enforcement and Intelligence Agents*, 30 J. OF COLLEGE AND U. L. 363, 379 (2004).

¹⁰ 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.

library records in response to overbroad, improperly issued, or unconstitutional requests for patron records.¹¹

The passage of the Patriot Act changed the landscape of legal process in the library. The debate about the Patriot Act has been public, vehement, and well-documented,¹² but the outcry has

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.” 3D CHARLES ALAN WRIGHT, NANCY J. KING & SUSAN R. KLEIN, *FEDERAL PRACTICE AND PROCEDURE: CRIMINAL* § 677 (3rd ed. 2004).

¹¹ 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.

¹² A search for Patriot Act in the same paragraph as libraries in Westlaw’s journals and law reviews database brings up 214 results. The same search in Lexis’s journals and law reviews database brings up 274 results. Comparable news searches were terminated for bringing up too many results. Searches performed on October 2, 2007. The public outcry about Section 215 has been judicially noted in *American Civil Liberties Union v. U.S. Dep’t. of Justice*, 321 F.Supp.2d 24, 32 (D.D.C.) (2004) [*ACLU II*].

diminished since the passage of the Patriot Reauthorization Acts.¹³ This article will discuss the various forms of post-Patriot Act process, how they 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 Patriot Act,¹⁴ but there are many statutory problems affecting civil liberties that still need to be addressed. There is still plenty of opportunity for advocacy.

Section 215 – The Library Provision

The original focus of the debate for librarians was Section 215.¹⁵ 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."¹⁶ The Patriot Act changed the type of business records that could be requested from the Foreign Intelligence Surveillance Court (FISC) from transportation-related

¹³ USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109- 177, 120 Stat. 192 (2006) [Reauthorization Act I]; USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. 109-178, 120 Stat. 278 (2006) [Reauthorization Act II].

¹⁴ See the discussion at page ___ *infra*. (where Section 215 Audit Report is discussed)

¹⁵ Patriot Act, § 215, 115 Stat. at 287-88 (amending 50 U.S.C. §§ 1861-1863 (2000)).

¹⁶ Office of the Inspector General, United States Department of Justice, *A Review of the Federal Bureau of Investigation's Use of Section 215 Orders for Business Records*, Mar. 2007 [Section 215 Audit Report], <http://www.usdoj.gov/oig/special/s0703a/final.pdf>, at 8.

business records to the records of any business – including libraries.¹⁷ The pre-Patriot Act section on records that could be requested from the FISC clearly had no effect on libraries. 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.¹⁸ Section 215 allowed government fishing expeditions for information from physical library records such as circulation records or internet use sign up sheets or for computer search histories from library computers or servers, and the library community responded in force.

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 a return to pre-Patriot Act standards for issuing an order, which required that the order be about a specific person who is strongly suspected of terrorism,¹⁹ instead of the post-Patriot Act standard that "the records concerned are sought for an authorized investigation..."²⁰ Although the Senate version of the Reauthorization Act did

¹⁷ Note 13, *supra*, at 50 U.S.C. § 1861 (2001 Supp.).

¹⁸ *Id.* at 50 U.S.C. §§ 1861(d), 1862 (2001 Supp.).

¹⁹ 18 U.S.C. § 1862(b)(2)(B) (2000): "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."

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

contain language requiring more particularized statements regarding the target of the order,²¹ the compromise language that actually passed only added a weak relevancy standard: the records have to be relevant to an authorized investigation.²² 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.²³ Under this broad standard, it's 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 has sought or obtained tangible things under this section.²⁴

The language precluded the right to consult an attorney, since an attorney is rarely the "person necessary to produce the tangible things." The Reauthorization Act I addressed this problem,

²¹ See S. 1389, §7, 109th Cong. (2006). The Senate-passed version of Reauthorization Act I 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.

²² Reauthorization Act I, § 106(b)(2)(A), 120 Stat. at 196, to be codified at 50 U.S.C. § 1861 (b)(2)(A).

²³ *Id.*

²⁴ 50 U.S.C. 1861(d)(1) (Supp. 2002).

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.²⁵

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.²⁶

The Reauthorization Act I added judicial review provisions for Section 215 orders by FISC judges.²⁷ 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."²⁸ So the order can't be modified because it is onerous, oppressive, or overbroad. The non-disclosure requirement can't be challenged until a year after the order to produce has been issued.²⁹ 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

²⁵ Reauthorization Act I, § 106(e), 120 Stat. at 197, 120 Stat. at , to be codified at 50 U.S.C. 1861(d)(1)(B).

²⁶ Reauthorization Act II, § 4, 120 Stat. At 280, to be codified at 50 U.S.C. 1861(d)(2)(C).

²⁷ Reauthorization Act I, §106 (f)(2), 120 Stat. at 198, to be codified at 50 U.S.C. 1861(f).
Review of a petition challenging a Section 215 order shall be conducted *in camera*.

Reauthorization Act I, §106 (f)(2), 120 Stat. at 198, to be codified at 50 U.S.C. 1803(e)(2).

²⁸ *Id.*, to be codified at 50 U.S.C. 1861(f)(2)(B).

²⁹ Reauthorization Act II, § 3, 120 Stat. at 278-79.

frivolous.³⁰ 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.**³¹

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 bound by the gag order for another year.³²

There are serious constitutional problems with this scenario. The gag order imposes 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 Patriot Act, the government has consistently denied it ever engaged in,³³ or discuss the profound effect the gag order has on the recipients’

³⁰ *Id.*

³¹ Reauthorization Act I, § 106(f), 120 Stat. at 198, to be codified at 50 U.S.C. 1861(f)(2)(c)(i) (emphasis added).

³² *Id.*, to be codified at 50 U.S.C. 1861(f)(2)(c)(ii).

³³ See, e.g., John Ashcroft, *Protecting Life and Liberty* (Sept. 18, 2003):

“The Department of Justice has neither the staffing, the time nor the inclination to monitor the reading habits of Americans. No offense to the American Library Association, but we just don't

business or personal life.³⁴ The gag order 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. In invalidating a similar³⁵ non-disclosure provision imposed on recipients of national security letters, the district court stated:

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 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.).³⁶

care;” and 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. Wednesday, Dec. 14, 2005; Page A29.

³⁴ Responding to the Inspector General’s Improper Use of National Security Letters by the FBI, Hearing Before the Subcomm. on the Constitution, S. Comm. on the Judiciary, 110th Cong. 193 (2007) (statement of George Christian). [Christian Statement].

³⁵ Although there are substantive differences between the two non-disclosure provisions, as discussed more fully at _____, *infra*, none of those differences militate in favor of the constitutionality of Section 215. The two main differences are that NSL recipients don’t have to wait for a year to challenge the non-disclosure order, and that the imposition of the non-disclosure order is not automatic. Reauthorization Act I, § 116, 120 Stat. at 213-17, to be codified at 18 U.S.C. 2709 (c) and § 115, 120 Stat. at 211-13, to be codified at 18 U.S.C. 3511, respectively.

³⁶ *Doe v. Gonzales [Doe III]*, 500 F.Supp.2d 379, 421 (S.D.N.Y. 2007).

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.³⁷ In the context of national security letters, one court has found that such a constraint on judicial review of legislation that affects the First Amendment is so severe, it violates the constitutional provisions of checks and balances and separation of power.³⁸ And critics of this section wanted review of Section 215 orders in the federal district courts.³⁹ 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. Requests 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," only three of the highest level employees have the authority to make an application to the FISC.⁴⁰ Because of the controversy about the use of

³⁷ Reauthorization Act I, § 106 (f), 120 Stat. at 197, to be codified at 50 U.S.C. 1861 (f)(2)(c)(ii).

³⁸ *Doe III* at 411-16, see discussion, *infra*, at .

³⁹ S. 2088, 110th Cong. (2007) attempts to address this issue, by adding provisions allowing federal district courts **and** FISA courts to hear petitions.

⁴⁰ Reauthorization Act I, §106(a)(2), 120 at .196, to be codified at 15 U.S.C. 1861(a)(3).

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.⁴¹

The Reauthorization Act I added more congressional oversight of Section 215 orders and increased the reporting requirements.⁴² Before the Reauthorization Acts, the total number of

⁴¹ Section 215 Audit Report, *supra*, note 15, at . In a University of Illinois study in 2003, at least two librarians reported that they had received court orders prohibiting them from telling patrons that authorities requested information, and two librarians indicated that they did not answer some of the questions about service of an order because they believed they were legally prohibited from doing so. Library Research Ctr., Univ. of Ill. at Urbana-Champaign, *Public Libraries' Response to the Events of 9/11/2001: One Year Later*,

<http://lrc.lis.uiuc.edu/web/PLCLnum.pdf> (last visited Nov. 13, 2007). (553 libraries responded; see Leigh S. Estabrook,

The Response of Public Libraries to the Events of September 11, 2001, 84 Ill. Libr. 1 (2002), also available at

http://www.cyberdriveillinois.com/publications/pdf_publications/illlibrary_v84_n1.pdf.)

In conversation with lawyers I have had, most lawyers 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.

⁴² Reauthorization Act I, §106(h)(2), 120 Stat. at 199, to be codified at 50 U.S.C. §

Section 215 orders and the total number of Section 215 orders that requested library or bookstore records had been the subject of highly contested litigation.⁴³

1862(b)(3).

⁴³ There have so far been six cases - four reported and two unreported - that have addressed Section 215 since the passage of the Patriot Act. The reported cases are: *American Civil Liberties Union v. U.S. Dep't. of Justice*, 265 F. Supp.2d 20 (D.D.C. 2003) [*ACLU I*]; *American Civil Liberties Union v. U.S. Dep't. of Justice*, 321 F.Supp.2d 24 (D.D.C.), 2004) [*ACLU II*]; *Electronic Privacy Information Center v. Dep't. of Defense*, 355 F.Supp.2d 98 (D.D.C. 2004) (plaintiff's request for expedited FOIA processing was denied, given lack of evidence of any current public interest in datamining software for antiterrorism program, as opposed to general subject of "data mining."); and *Muslim Community Ass'n. of Ann Arbor v. Ashcroft*, 459 F.Supp.2d 592 (E.D. Mich. 2006) (Muslim groups challenged the constitutionality of Section 215, alleging that it chilled their First Amendment rights; the lawsuit survived the government's standing challenge, but after the Reauthorization Acts amended Section 215, the ACLU withdrew the complaint). The unreported cases are: *American Civil Liberties Union v. U.S. Dep't. of Justice*, No. C-04-4447, 2005 WL 5888354; 2005 U.S. Dist. LEXIS 3763 (N.D. Cal. 2005) (ACLU FOIA request need not be processed on an expedited basis); and *Gerstein v. C.I.A.*, No. C-06-4643, 2006 WL3462658; 2006 U.S. Dist. LEXIS 89883 (N.D. Cal. 2006)(request for expedited FOIA processing of documents relating to unauthorized disclosure of classified documents was denied).

Litigating Section 215 – the Public’s Right to Know How the Patriot Act Has been Utilized.

Section 215 litigation has primarily involved Freedom of Information Act (FOIA) requests.⁴⁴ *ACLU I* and *ACLU II* are the cases that directly address the public's right to know about the use of Section 215. In *ACLU I*, the ACLU filed suit to compel the Department of Justice (DOJ) to respond to a Freedom of Information Act (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."⁴⁵ The public debate about the effect of the 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 have been used."⁴⁶

Some information about aggregate statistics had been released to Congress in a classified form,⁴⁷ and some of it was released only after Congressional threats.⁴⁸ *ACLU I* was heard in the

⁴⁴ *Supra*, note 43; the exception is *Muslim Community Ass'n. of Ann Arbor v. Ashcroft*, a direct First Amendment challenge to Section 215.

⁴⁵ *ACLU I*, at 25.

⁴⁶ *Id.*

⁴⁷ *Id.* at 24-25.

D.C. Circuit, notoriously extremely deferential to claims of national security.⁴⁹ 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 aggregate statistical data to the public in only one category (orders approving electronic surveillance) but had limited the dissemination of other aggregate statistical information. The court rejected the ACLU's argument that mere publication of aggregate statistical information could not of itself harm national security, or Congress wouldn't have authorized it for any type of Patriot Act surveillance. And the court also rejected the ACLU's argument that Congress was trying pretty hard to get this aggregate information to the

⁴⁸ Congress's attempts to secure information about the implementation of the Patriot Act have been numerous and only partially successful *See* FBI Oversight in the 107th Congress. Senate Judiciary Committee: FISA Implementation Failures, an Interim Report by Senators Patrick Leahy, Charles Grassley & Arlen Specter [Leahy Report] (Feb. 2003) (www.fas.org/irp/congress/2003_rpt/fisa.pdf) (at pages 9-10) Some answers were provided only after a threat to subpoena the Attorney General. (*Ashcroft Threatened with Hill Subpoena*, Washington Times, Aug. 21, 2002. The Leahy Report concluded: "The Congress and the **American people deserve to know what their government is doing.** *Id.* at 10 (emphasis added).

⁴⁹ Nathan Slegers, Note, *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 (2006).

American people.⁵⁰ Then the Attorney General voluntarily declassified the number of times the government had used Section 215, declaring:

This memorandum confirms I have declassified the number of times to date the Department of Justice, including the Federal Bureau of Investigation (FBI), has utilized Section 215 of the USA PATRIOT Act relating to the production of business records. The number of times Section 215 has been used to date is zero (0)... While Congress has regularly been informed regarding the number of times Section 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 Section 215. Consequently, I have determined that it is in the public interest and the best interest of law enforcement to declassify this information.⁵¹

The ACLU filed *ACLU II* after a new FOIA request 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. 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

⁵⁰ See Plaintiff's Cross-Motion for Summary Judgment, at 6, <http://www.epic.org/privacy/terrorism/usapatriot/foia/sj-memo.pdf>; Leahy Report at 5, 13.

⁵¹ Memorandum for Director Robert S. Mueller (available at <http://www.cdt.org/security/usapatriot/030918doj.shtml>) The memorandum was issued in September 18 2003. (See e.g., *ACLU II* at 25 and the declaration of David M. Hardy, page 5, attached to motion for partial summary judgment filed by the government in 03-2522 defendants' summary judgment motion, exhibit B, attachment 2, in *ACLU II*.)

adversaries to conduct their intelligence or international terrorist activities more securely.”⁵² The court found that the number of applications would reveal the level of FBI activity, which might “also 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.”⁵³ As the court in *Gerstein v. U.S. Department of Justice* pointed out, making a claim that statistical information about past practices would be a “road map” for future efforts to be aimed at purported disclosed weaknesses is “dubious” logic, as past practices “are hardly a reliable indicator that [the government] will continue to do so.”⁵⁴

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 granted as requested, granted as modified, or denied:”

⁵² *ACLU II*, at 6.

⁵³ *ACLU II*, at 36-37.

⁵⁴ No. C-03-04893, slip op. at 2 (N.D. Cal., 2005, denying plaintiff’s request for FOIA records for summary statistics on the use of Section 213 on other grounds.

the number of 215 orders either granted, modified, or denied for the production of each of the following: library circulation records, library patron lists, book sales records, or book customer lists; firearms sales records; tax return records; educational records; and medical records containing information that would identify a person.⁵⁵

The third provision is new, allowing Congress and the public access to information about the use of Section 215 in areas relating to privacy and other First Amendment rights. In addition, the Reauthorization Act requires the Office of the Inspector General (OIG) of the DOJ to conduct a comprehensive audit of DOJ procedures, to review the effectiveness of Section 215 authority and report any abuses.⁵⁶ That audit was released in March 2007.⁵⁷ The audit confirmed that Section 215 had not been used before 2004: a "pure" Section 215 order⁵⁸ was not approved until May, 2004, and a "combination" Section 215 order was first approved in February, 2005.⁵⁹ There had been a total of 21 applications for pure Section 215 orders from 2002 to 2005, but the first one that was approved was not until 2004. No combination

⁵⁵ Reauthorization Act, § 106(h)(2), 120 Stat. at 199-200, to be codified at 50 U.S.C. 1862(b)(3).

⁵⁶ Reauthorization Act I, § 106A, 120 Stat. at 200.

⁵⁷ Section 215 Audit Report, *supra*, note 16.

⁵⁸ According to the Office of Intelligence Policy and Review (OIPR), a "pure" Section 215 order is an application for tangible items that is "not associated with applications for any other FISA authority, while a "combo" application refers to a Section 215 order that was added to a request for a FISA pen register/trap & trace order. *Id.* at v-vi.

⁵⁹ Section 215 Audit Report, *supra*, note 15, at 17, 35.

applications were even sent in until 2005.⁶⁰ 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 below summarizes the changes that were made to Section 215 by the Patriot Act and the Reauthorization Acts.

	Before the PATRIOT Act	After the PATRIOT Act	After the Re-Authorization Act	Proposed in the 110 th Congress Issue
Records	None allowed; section 215 orders limited to the records of common carriers, public accommodation facilities, physical storage facilities or vehicle rental facilities. (50 U.S.C. § 1862 (2000)).	Any tangible things (including books, records, papers, documents and other items) could be requested from “any business or entity.” (50 U.S.C. §1861 (2002 supp.))	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 3 high level employees are empowered to sign the application (50 U.S.C. § 1861 (a)(3)) Records must be described with “sufficient particularity” to allow them to be identified.	
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	(50 U.S.C. 1861(b)(2)) An application must state that “the records concerned are sought for an authorized investigation	50 U.S.C. 1861(b)(2) (A) added the requirement that there be “ reasonable grounds to believe ” the records sought “ are relevant to an authorized investigation” but	S. 2088, § 9 revises the standard to more closely conform to the pre-Patriot Act version (specific and articulable facts

⁶⁰ See *infra*, at , for a discussion of the reasons Section 15 orders were not approved.

	<p>person to whom the records pertain is a foreign power or an agent of a foreign power.” (18 U.S.C. 1862, 2000)</p>	<p>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.”</p>	<p>that records are “presumptively relevant” if they that they pertain to “(i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.”</p>	<p>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).</p>
<p>Gag Order & Disclosure</p>	<p>Yes.</p>	<p>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. (50 U.S.C. 1861(d)</p> <p>No specified penalty (contempt of court)</p>	<p>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. See 50 U.S.C. 1861 (d)(1 No specified penalty (contempt of court)</p>	<p>S. 2088, § 9 requires specific and articulable facts why the non-disclosure agreement is necessary and how it is narrowly tailored. Last 180 days, unless extended.</p>
<p>Review of the Order</p>	<p>No</p>	<p>No</p>	<p>Yes, after one year, in the FISA court. Added 50 U.S.C.</p>	<p>S. 2088, § 10, allows review within 20 days</p>

			1861 (f). 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 a request to lift the gag order.	in FISA court or district court
Sunset	No	Yes, , on 12/31/2005, but reauthorized	Yes 12/31/2009	N/A

You can access a copy of a Section 215 order at

http://www.aclu.org/patriot_foia/2003/215formorder.pdf.

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.⁶¹

⁶¹ Section 215 Audit Report, *supra*, note 15, at 19, 23, 26, 35, 73-74).

One of the orders prepared but never presented was an application for an order for library records.⁶² The applicant's supervisor:

would not permit the request to go forward because of the political controversy surrounding Section 215 requests for information from libraries. The 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 OIPR and the Department would disapprove of the FBI seeking information from a library, especially since the FBI had not obtained its first Section 215 order.⁶³

When the field office was advised that the application would not be sent, the field office obtained the information through other investigative means.⁶⁴ The report does not say which other investigative means were used.

The Section 215 Audit Report found that the FBI was not really successful in getting 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.⁶⁵ And the OIG found that FBI agents just didn't understand the process for obtaining

⁶² The request for library records was submitted in November, 2003. *Id.* at 28) 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.

⁶³ *Id.* at 28.

⁶⁴ *Id.*

⁶⁵ *Id.* at 60-63.

a Section 215 order – agents just used other methods of getting the information – including NSLs, grand jury subpoenas, or other process that was faster than a Section 215 order.⁶⁶

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 Section 215 orders**” and “**the evidence showed no instance where the information obtained from a Section 215 order resulted in a major case development, such as the disruption of a terrorist plot.**”⁶⁷ The Section 215 Audit did note that the FBI began using Section 215 more broadly in 2006, and that use will be reviewed in the next audit.⁶⁸ But to date, 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 Patriot Act conferred.

What the Section 215 Audit Report did show was that political pressure by librarians was effective: no Section 215 orders were served on libraries.⁶⁹ But libraries and bookstores should

⁶⁶ *Id.* at 63-64.

⁶⁷ *Id.* at 79. The orders were used primarily to exhaust investigative leads, from driver’s license records, apartment leasing records, and credit card records. *Id.*

⁶⁸ *Id.* at 80.

⁶⁹ *Id.* 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 A. Nieland, Note, *National Security Letters and the Amended Patriot Act*, 92 CORNELL L. REV. 1201, 1226 (2007).

be exempted from the whole process. Section 215 orders are not as simple to secure as a search warrant, but are much more constitutionally suspect: the rational compromise would be to subject library and bookstore records to legal process where there is 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.

Although Section 215 was scheduled to sunset in 2005, the Reauthorization Act extended that sunset until December 2009.⁷⁰ The Section 215 Audit Report findings about 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-Patriot Act standards and types of records for this section when it comes up for review.

The Upstart Contender – National Security Letters

If the FBI hasn't been using Section 215 to get library records, what has the FBI been using? Contrary to John Ashcroft's assertion that the FBI isn't interested in what people were reading,⁷¹ we know that libraries' computer records have been the subject of Patriot Act

⁷⁰ Reauthorization Act I, §102(b), 120 Stat. at 195, editorially designated 50 U.S.C. 1801 note.

⁷¹ "The Department of Justice has neither the staffing, the time nor the inclination to monitor the reading habits of Americans. No offense to the American Library Association, but we just don't care." John Ashcroft, *Protecting Life and Liberty* (Sept. 18, 2003),

<http://www.usdoj.gov/archive/ag/speeches/2003/091803memphisremarks.htm>.

process, and that libraries have been asked for and provided library records.⁷² Since Section 215 orders were so difficult to obtain, NSLs may have provided an easy alternative for some kinds of information. An NSL is issued administratively by the agency -- it is not issued by a court.⁷³ 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 prior to releasing records.⁷⁴

The form of NSL that concerns libraries allows the government to request subscriber information or electronic communication transactional records from an “electronic

⁷² Sometimes the FBI just asked for library records, and was given the information voluntarily.

In a 2002 survey, 47% of the libraries responding voluntarily complied with informal law enforcement requests for information about patrons' reading habits and Internet preferences in the previous year. Library Research Ctr., Univ. of Ill. at Urbana-Champaign, *Public Libraries' Response to the Events of 9/11/2001: One Year Later*,

<http://lrc.lis.uiuc.edu/web/PLCLnum.pdf> (last visited Nov. 13, 2007). *See also*, Dan

Mihalopoulos, *Suit Contests Anti-Terror Patriot Act*, CHI. TRIB., Jul. 31, 2003, at 10: “An FBI official said Wednesday that Patriot Act powers have been employed about 50 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.”

⁷³ 18 U.S.C. 2709 (1996).

⁷⁴ For a general discussion of the evolution of national security letters, see Andrew A. Nieland, Note, *National Security Letters and the Amended Patriot Act*, 92 CORNELL L. REV. 1201, 1206-1211 (2007).

communication service.”⁷⁵ 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” required to comply with a national security letter: “‘electronic communication service’ means any service which provides to users thereof the ability to send or receive wire or electronic communications.”⁷⁶

Despite this statutory language, NSLs were not the main focus for critics of 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.⁷⁷ When an anonymous internet service provider was served with an NSL in 2004, and

⁷⁵ Patriot Act § 505(a), 115 Stat. At 365-66, codified at 18 U.S.C. § 2709 (a), (b) (2000)).

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.**” (emphasis added). *Doe v. Ashcroft*, [*Doe I*], 341 F.Supp.2d 471, 480 (S.D.N.Y. 2004).

⁷⁶ 18 U.S.C. § 2510(15) (2000).

⁷⁷ *They Rose to the Challenge: Public Librarians Take on the USA Patriot Act Through Doe v. Gonzales*, George Christian, presentation at the American Association of Law Libraries Annual Meeting, New Orleans, July 14, 2007 [*They Rose to the Challenge*]. The author’s library has such a program on its public computers.

filed suit to protest the non-disclosure provisions,⁷⁸ the debate about NSLs heated up. The attention of the library community was 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 Patriot Act.⁷⁹ 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.”⁸⁰

NSLs may be issued to request “subscriber information and toll billing records information, or electronic communication transactional records.”⁸¹ Before the 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.”⁸² That standard was lessened by the 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

⁷⁸ *Doe I*, see discussion *infra* at

⁷⁹ *Doe II*, see discussion *infra* at

⁸⁰ *They Rose to the Challenge*, *supra*, note 77. The consortium understood the FBI’s request to mean that **all** records from the relevant time period were being requested. *Id.* The copy of the NSL served on the Connecticut library consortium can be reviewed at http://www.aclu.org/images/nationalsecurityletters/asset_upload_file924_25995.pdf.

⁸¹ 18 U.S.C. 2709(a) (2000). This section was not revised by the Reauthorization Acts.

⁸² 18 U.S.C. 2709(b)(1)(B) (2000).

States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.”⁸³

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:

That 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 websites visited. [citations omitted] Information requested by NSLs issued pursuant to § 2709 can also reveal the identity of an internet user associated with a certain email address, Internet Protocol address, or screen name.⁸⁴

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,

⁸³ Patriot Act, § 505, 115 Stat. At 365-66, amending 18 U.S.C. 2709(b)(1)(B). And the Patriot Act expanded FBI issuing authority beyond FBI headquarter officials to include the heads of the FBI field offices. NSLs always had a gag order, and there never has been a sunset provision for NSLs. *Id.* 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) (Supp. II 2002).

⁸⁴ *Doe III*, *supra*, note 36, at 387.

whether the request was “in the course of an authorized investigation,”⁸⁵ whether or not the recipient is a non-U.S. person or a U.S. person, and whether the investigation fully or partially implicates First Amendment activities. No other branch of the government reviews this part of the process.⁸⁶

The Pre-Reauthorization Act Cases – Doe I and Doe II

There has already been a fair amount written about the first two cases to ever challenge a national security letter, but a brief review is necessary to set the stage for the debate about the Reauthorizations Acts and the changes that were made to the NSL provisions.⁸⁷

Doe I was filed by a still-unknown internet service provider (ISP), alleging that the NSL statute violated the First, Fourth and Fifth Amendments to the Constitution.⁸⁸ The District Court found

⁸⁵ Office of the Inspector General, United States Department of Justice, *A Review of the Federal Bureau of Investigation’s Use of National Security Letters* [NSL Audit Report], Mar. 2007, at 121-24,

<http://www.usdoj.gov/oig/special/s0703b/final.pdf>.

⁸⁶ This lack of review has been a focus of criticism of NSLs. See pages , *infra*.

⁸⁷ 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); *National Security Letters and the Amended Patriot Act*, *supra*, note 69, at 1215-1224.

that the NSL statute prohibited the recipient from consulting an attorney,⁸⁹ was coercive to the reasonable recipient,⁹⁰ imposed a permanent prior restraint on speech in violation of the First Amendment,⁹¹ and improperly precluded judicial review.⁹² While the Fourth Amendment does not preclude issuing administrative subpoenas, there are Fourth 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.⁹³ 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.⁹⁴ The Court enjoined the government from enforcing the NSL provisions, but stayed the injunction to allow the government to appeal.⁹⁵

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

⁸⁸ *Doe I*, *supra*, note , vacated and remanded *sub nom.* *Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006).

⁸⁹ *Id.*, at 496.

⁹⁰ *Id.* at 503.

⁹¹ *Id.* at 512.

⁹² *Id.* at 506.

⁹³ *Id.* at 495-96.

⁹⁴ *Id.* at 526-27.

⁹⁵ *Id.*

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 at the time, during the period when Congress was debating the Reauthorization Acts.⁹⁶ The court in *Doe I* had this to say about the scope of the gag order in Section 2709:

... the 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.**⁹⁷ (emphasis added).

The government did appeal and the gag order remained in place during the national debate on reauthorizing the Patriot Act; the government was successful in stifling dissent.⁹⁸ The anonymous 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.⁹⁹

⁹⁶ Anonymous, *My National Security Letter Gag Order*, Mar. 23, 2007, Washintonpost.com, <http://www.washingtonpost.com/wp-dyn/content/article/2007/03/22/AR2007032201882.html>.

⁹⁷ *Doe I*, at 519.

⁹⁸ *My National Security Letter Gag Order*, *supra*, note 96.

⁹⁹ See *Doe III*, *supra* note 36, at 426. The government dropped its request for the information in November, 2006. *My National Security Letter Gag Order*, *supra*, note 96.

In the second lawsuit to challenge NSLs, a Connecticut library consortium¹⁰⁰ 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 Patriot Act.¹⁰¹ The District Court's decision enjoined the government from enforcing the nondisclosure provision of section 2709(c) to the extent the provision prevented the recipient from revealing its identity as a recipient of an NSL, holding that 2709(c) did not satisfy the requisite First Amendment strict scrutiny test, as it was not narrowly tailored to serve a compelling state interest.¹⁰² Again, the injunction was stayed to allow the government to appeal.¹⁰³

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,¹⁰⁴ the plaintiffs in Doe II were still governed by a gag order while the government appealed the District Court order, and were

¹⁰⁰ 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." Christian Statement, *supra*, note 34.

¹⁰¹ Doe v. Gonzales, 386 F.Supp.2d 66 (D. Conn. 2005) [Doe II]. At the time the consortium was served, the decision in Doe I had been issued.

¹⁰² Doe II at 82.

¹⁰³ *Id.*

¹⁰⁴ Alison Leigh Cowan, *A Court Fight to Keep a Secret That's Long Been Revealed*, N.Y. TIMES, Nov. 18, 2005, at B1.

similarly prevented from participating in the public debate about NSLs that had been taking place during the hearings on the Reauthorization Acts.¹⁰⁵

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 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 2007, Mr. Christian was eloquent about the need for libraries to continue their measured and thoughtful resistance to government fishing expeditions for library records.¹⁰⁶ The NSL he was served was not for material the FBI needed urgently – the NSL wasn’t even delivered until almost two months after it was written.¹⁰⁷ 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.¹⁰⁸ The consortium needed the FBI’s

¹⁰⁵ See *Doe v. Gonzales*, 449 F.3d 415 (2nd Cir. N.Y. 2006). [*Doe III*] This is the opinion on the consolidated appeals in *Doe I* and *Doe II*.

¹⁰⁶ *They Rose to the Challenge*, *supra*, note 77; Christian Statement, *supra*, note 34. 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 pleadings that the government attempted to redact for national security purposes were portions of United States Supreme Court decisions. *They Rose to the Challenge*, *supra*, note 77.

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

permission to even consult with an attorney.¹⁰⁹ 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.¹¹⁰ 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 knew who the plaintiffs were:

the government argued that merely revealing ourselves as recipients of a national security letter would violate national security. Our 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 our 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 our attorneys had submitted remain under seal in court papers.

Even though our names were not thoroughly redacted from the court documents, the government did redact from our affidavits our claim that 48 states had laws protecting the privacy of patron library records. We could not understand the threat to national security this information posed, but we did note that Attorney General Gonzales claimed to Congress that there was no statutory justification for claims of privacy.¹¹¹

¹⁰⁹ Christian Statement, *supra*, note 44.

¹¹⁰ *Doe v. Gonzales*, 546 U.S. 1301 (2005), declining to lift gag order; the gag order was not lifted until May, 2006. *Doe v. Gonzales*, 449 F.3d at 421.

¹¹¹ *They Rose to the Challenge*, *supra*, note 77.

The government even tried to redact “direct quotes from Supreme Court opinions that undercut the government’s arguments in the case.”¹¹² 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.¹¹³

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).¹¹⁴ The government had successfully used the specter of national security to prevent dissent and stifle free speech, not to protect the public from terrorism.

The Reauthorization Acts Changed the Patriot Act NSL Provisions On Nondisclosure, Judicial Review, Libraries, and Oversight.

The Reauthorization Act I amended the blanket prohibition on disclosure imposed by the

¹¹² ACLU Press Release, Aug. 8, 2006,

<http://www.aclu.org/safefree/nationalsecurityletters/26404prs20060807.html>

¹¹³ *Id.*; *U.S. v. U.S. Dist. Court for Eastern Dist. of Michigan*, 407 U.S. 297, 314 (1972).

¹¹⁴ *Doe v. Gonzales*, 449 F.3d at 421.

Patriot Act.¹¹⁵ 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 counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person.”¹¹⁶ 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*, there is no reason to assume that the non-disclosure certification will not be routinely included in NSLs. There are new guidelines for issuing NSLs, which indicate “that in most situations non-disclosure will be appropriate.”¹¹⁷

If there is a non-disclosure certification, then the recipient may not disclose the NSL to anyone except these 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.¹¹⁸ So the right to consult with an attorney is now explicit. And the recipient of an NSL has to inform anyone who is told of the NSL of the non-disclosure requirements.¹¹⁹ A specific penalty for

¹¹⁵ 18 U.S.C. 2709(c) (Supp. I 2001).

¹¹⁶ Reauthorization Act I, § 116, 120 Stat. at 213-17, to be codified at 18 U.S.C. 2709(c).

¹¹⁷ Comprehensive Guidance on National Security Letters, Federal Bureau of Investigation, June 1, 2007, http://epic.org/privacy/nsl/New_NSL_Guidelines.pdf, at 12.

¹¹⁸ Reauthorization Act II, § 4, 120 Stat. at 280-81, to be codified at 18 U.S.C. 2709 (c)(4).

¹¹⁹ Reauthorization Act I, § 116, 120 Stat. at 213-17, amending 18 U.S.C. 2709(c) (3).

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 both.¹²⁰

Judicial Review

The Reauthorization Act I added judicial review of the scope of an NSL, by allowing the recipient to file a petition in the federal district court for an order to modify or set aside the NSL.¹²¹ The government now has the means to enforce an NSL by requesting a court order to compel compliance.¹²² All proceedings regarding NSLs are closed.¹²³

A recipient may also file petition to modify or set aside the nondisclosure requirement.¹²⁴

If the petition is filed within one year of the issuance of the NSL, the court can modify the

¹²⁰ Reauthorization Act I, § 117, 120 Stat. at 217, amending 18 U.S.C. 1510(e). (emphasis added) (the fine is \$250,000 for an individual and \$500,000 for an entity. 18 U.S.C. 3571, 3559 (2000).

¹²¹ Reauthorization Act 1, §115, 120 Stat. at 211-12, adding new 18 U.S.C. 3511.

¹²² *Id.*, adding new 18 U.S.C. 3511(c).

¹²³ *Id.*, adding new 18 U.S.C. 3511(d).

¹²⁴ *Id.*, adding new 18 U.S.C. 3511(b).

nondisclosure 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,...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.**¹²⁵

The “enumerated harms”¹²⁶ 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.

If the petition to modify the nondisclosure 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 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 re-certification is

¹²⁵ *Id.*, adding new 18 U.S.C. 3511(b)(2). (emphasis added).

¹²⁶ *Doe III, supra*, note 36, at 389 collectively refers to the conditions in the statute as the “enumerated harms.”

conclusive, unless it is made in bad faith.¹²⁷ If the government recertifies, the recipient of the gag order has to wait another year to request termination of the order.

The number of reasons to get and maintain a gag order is broad, and includes 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.

The Library Exemption

The 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).”¹²⁸ Since Section 2510(15) defines an “electronic service provider” as any “service which provides users thereof with the ability to send or receive wire or electronic communications,” the exception may be so broad 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 internet service provider, 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 Government will

¹²⁷ Reauthorization Act I, § 115, 120 Stat. at 211-12, adding new 18 U.S.C. 3511(b)(3).

(emphasis added).

¹²⁸ Reauthorization Act II, § 5, 120 Stat. at 281, to be codified at 18 U.S.C. 2709(f).

need a court order to seize library records for foreign intelligence purposes.”¹²⁹ John Conyers disagreed, stating that the exemption was nothing but a “fig leaf.”¹³⁰ 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.”¹³¹

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. The scope of the exemption remains to be litigated.

The chart below summarizes the changes made in NSLs by the Patriot Act and the Reauthorization Acts:

¹²⁹ 152 CONG. REC. S1558 (Mar. 1, 2006) (Statement of Sen. Leahy).

¹³⁰ 152 CONG. REC. H585 (Mar. 7, 2006) (Statement of Rep. Conyers)

¹³¹ Christian Statement, *supra*, note 44.

18 U.S.C. 2709	Before the PATRIOT Act	After the PATRIOT Act	After the Re-Authorization Act	Proposals in the 110th Congress
Records	Subscriber information, toll billing records, electronic communications transactional records. By its terms, the statute covers “identified customer’s name, address, length of service, and billing information”	The same	The same	H.R. 3189 prohibits letters containing unreasonable requirements or requiring privileged material.
Standard to Issue	Specific and articulable facts that the person or entity to whom information sought pertains is a foreign power or an agent of a foreign power	Certify the records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, (if not conducted solely on the basis of activities protected by the first amendment for a U.S. person). So you don’t have to be the subject of a national security investigation to have your records produced pursuant to an NSL.	The same	H.R. 1739 would add the "specific and articulable facts" standard in addition to the two criteria added by the Patriot Act. S. 2088 would allow an NSL to issue only where the records relate to an "ongoing, authorized, and specifically identified national security investigation: and returns to the "specific and articulable facts" standard. H.R. 3189 requires the specific facts standard and retains the 1st Amendment prohibition.
Gag Order & Disclosure	Yes (no specific penalty/contempt of court)	Yes (no specific penalty/contempt of court)	Yes; penalty under 18 U.S.C. 1510 (e) of up to 5 years and fine of \$25,000 for an individual and \$500,000 for an organization; may consult attorney	H.R. 1739 would make an A.G. certification that disclosure will endanger the national security or interfere with diplomatic relations a rebuttable presumption, not a conclusive finding. H.R. #189 limits

				disclosure gag to 30 days,
Review of the Order	No	No	Yes; 18 U.S.C. 3511. Judicial review in federal court; see Doe v. Gonzales, 449 F.3d 415 (2006)	H.R. 3189 authorizes judicial review for modification or revocation of a letter, and adds ability to suppress evidence and for civil action for misuse of letters. S. 2088 revises criteria for judicial review of nondisclosure orders.
Library Section	No	No	Yes. Libraries that offer use of the internet to patrons may not be are not “electronic communication service providers” Unless they provide the services listed in 18 U.S.C.A. 2510(15) which is so broad it appears to swallow the exemption.	Libraries that are part of institutions that host internet services (see 18 U.S.C. 2510(15)) are clearly not exempt under this section (academic, firm law libraries). Public library exemption still subject to dispute, since all provide internet services. Legislative history does not resolve the issue.
Sunset	N/A	N/A	N/A	After 5 years, H.R. 3189 would require a reversion to law as it existed on October 25, 2001. S. 2008 would terminate come authority for issuing NSLs on December 31, 2009.

The NSL Audit Report

The Reauthorization Acts expand Congressional oversight of NSLs¹³² and call for an Inspector General’s audit of use of the authority.¹³³ In March 2007, the Inspector General released its report of the use of NSLs for the years 2003 through 2005.¹³⁴ 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.

Use of NSLs has increased dramatically, expanding from 8,500 requests in 2000 to 47,000 in 2005.¹³⁵ Because of poor or non-existent record keeping, the FBI’s database records “significantly understates the number of FBI NSLs,” but the total number listed as issued from 2003 through 2005 is 143, 047.¹³⁶ Based on the NSL Audit Report’s sample study of case files, the numbers in the database are underreported by 17%.¹³⁷ Because of “delays in uploading NSL data and the flaws in the OGC¹³⁸ database, the total numbers of NSL requests

¹³² Reauthorization Act I, § 118, 120 Stat. at 217-18, to be codified at 15 U.S.C. 1681v(f).

¹³³ Reauthorization Act I, § 119, 120 Stat. at 219-21.

¹³⁴ NSL Audit Report, *supra*, note 85.

¹³⁵ *Id.* at 120.

¹³⁶ *Id.* at xviii.

¹³⁷ *Id.* at xvi.

¹³⁸ The OGC is the FBI’s office of General Counsel National Security Letter database.

Id. at xv.

that were reported to Congress semiannually in CYs 2003, 2004, and 2005 were significantly understated.”¹³⁹

During the three years under review, the percentage of NSLs used to investigate “United States persons” increased from 39% in 2003 to 53% in 2005.¹⁴⁰ The NSL Audit Report also found that in 12% of the case files examined, the investigative target of the NSL described a non-United States person when the target was, in fact, a United States person.¹⁴¹ So in those cases, the FBI was able to ignore the First Amendment restrictions imposed on targeting United States persons.”¹⁴²

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.”¹⁴³ And the NSL Audit Report found that the only FBI data collection system

¹³⁹ *Id.* at xvii.

¹⁴⁰ *Id.* at 38.

¹⁴¹ *Id.* at xlv-xlvi.

¹⁴² 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 on the basis of activities protected by the first amendment.” 18 U.S.C. 2709 (b)(2) (2000).

¹⁴³ NSL Audit Report, *supra*, note 85, at 124.

produced “inaccurate” results¹⁴⁴ and a “significant number of NSL-related possible violations are not being identified or reported” as required.¹⁴⁵ **Sixty percent** of the individual files examined “contained one or more violations of FBI internal control policies relating to national security letters.”¹⁴⁶ The FBI regularly issued NSLs in such a way that there was no mechanism to insure that the NSLs were issued in the course of authorized investigations or to determine whether the information sought in the NSLs was relevant to those investigations.¹⁴⁷ In other words, NSLs could be and were issued for records regardless of their nexus to national security investigations.

The DOJ’s own audit, of a much larger sample than the NSL Audit Report found similar numbers of misuses of orders, according to FBI General Counsel Valerie Caproni.¹⁴⁸ And the FBI’s most recent review indicates that, in fact, the FBI “improperly used national security

¹⁴⁴ *Id.* at 121.

¹⁴⁵ *Id.* at 84, 123. The NSL Audit Report found that 22% of the files reviewed contained unreported NSL-related possible violations. *Id.*

¹⁴⁶ *Id.* at 123-124.

¹⁴⁷ *Id.* at 86, 123.

¹⁴⁸ John Solomon, *FBI Finds It Frequently Overstepped in Collecting Data*, WASH. POST, June 14, 2007, at A1, available at <http://www.washingtonpost.com/wp-dyn/content/article/2007/06/13/AR2007061302453.html>: “The FBI’s comprehensive audit of National Security Letter 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 10% 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.*

letters in 2006 to obtain personal data on Americans during terror and spy investigations.¹⁴⁹

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 couldn't be bothered to meet its own minimal standards. For those situations, the agency used exigent letters.

Exigent Letters

One of the problems the NSL Audit Report revealed was the use of exigent letters to get information before an NSL was issued.¹⁵⁰ 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**.¹⁵¹ 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 red Acted] as expeditiously as possible.¹⁵²

¹⁴⁹ Lara Jakes Jordan, *FBI Chief Says Report Will Show Additional Improper Use of Subpoenas in Terror, Spy Cases*, LAW.COM, <http://www.law.com/jsp/article.jsp?id=1204716628871>, Mar. 5, 2008, quoting FBI Director Robert Mueller. The report is a follow-up to the earlier report. *Id.*

¹⁵⁰ NSL Audit Report, *supra* note 85, at 86.

¹⁵¹ *Id.* at 86, 89.

¹⁵² *Id.* at 89.

The language of the letters could just as easily apply to providing an IP address as telephone number. The 739 letters requested information on about 3,000 different telephone numbers.¹⁵³ The service providers turned over records without ever receiving the NSL,¹⁵⁴ or turned over more information than the FBI requested.¹⁵⁵ A service provider who knowingly or intentionally violates the prohibition is subject to civil liability, but there are no criminal penalties for the breach.¹⁵⁶ 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 2004.¹⁵⁷ 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.”¹⁵⁸ The PCLO Board’s role is to advise and oversee. As part of its first statutory report, the PCLO Board reviewed the OIG

¹⁵³ *Id.* at 90.

¹⁵⁴ *Id.*

¹⁵⁵ *FBI Finds It Frequently Overstepped in Collecting Data*, *supra*, note 148.

¹⁵⁶ 18 U.S.C. 2707 (Supp. I 2002).l

¹⁵⁷ Intelligence Reform and Terrorism Prevention Act of 2004 § 1061, 5 U.S.C. § 601 note (Supp. IV 2006), editorially designated 42 U.S.C. 2000ee.

¹⁵⁸ *Id.*, at 42 U.S.C. 2000ee(c).

report regarding the FBI's use of NSLs.¹⁵⁹ The PCLO Board is going to issue its own recommendations for solving the problems, but in the meantime, 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.

The OIG agrees, and in its latest report to Congress, in which the goals for the Department of Justice 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.¹⁶⁰

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."

¹⁶¹ For the DOJ, "striking the appropriate balance between meeting its critical

¹⁵⁹ Privacy and Civil Liberties Oversight Board: First Annual Report to Congress, March 2006 - March 2007, <http://www.privacyboard.gov/reports/2007/congress2007.pdf>, at iv.

¹⁶⁰ Office of the Inspector General, Semiannual Report to Congress, April 1, 2007-September 30, 2007, <http://www.usdoj.gov/oig/semiannual/0711/challenges.htm>.

¹⁶¹ *Id.*

counterterrorism-related responsibilities and respecting civil rights, civil liberties, and privacy rights remains a key challenge...”¹⁶²

And the FBI hasn’t or can’t prove by specific example that the current use of NSLs results in timely and useful intelligence. When the PCLO Board issued its second annual report, there was harsh criticism of the FBI’s ability to defend the use of NSLs in their present form:

...the 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.¹⁶³

Doe III – The NSL Statute Still Violates the Constitution

Since some of the changes that were made to the NSL provisions directly addressed 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.¹⁶⁴ Judge

¹⁶² Office of the Inspector General, *Top Management and Performance Challenges in the Department of Justice – 2007*, <http://www.usdoj.gov/oig/challenges/2007/index.htm>.

¹⁶³ Privacy and Civil Liberties Oversight Board: Second Annual Report to Congress, March 2007 – January 2008, <http://www.privacyboard.gov/reports/2008/congress2008.pdf>, at 24.

¹⁶⁴ *Doe III*, *supra*, note 36, at 385-86.

Marerro ruled that the changes made to the law by the Reauthorization Acts were insufficient to insulate NSLs from First Amendment and separation of powers challenges.¹⁶⁵

The *Doe III* court held that the revised nondisclosure provisions, which allow 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 Amendment.¹⁶⁶ The court noted that:

Unfortunately, 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.¹⁶⁷

The District Court also held that the standards prescribed by Congress for judicial review of the non-disclosure orders “is plainly at odds with First Amendment jurisprudence which requires

¹⁶⁵ *Id.* at .

¹⁶⁶ *Id.* at 425: Section 2709 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.”

¹⁶⁷ *Id.* at 397-398. In support of its opinion, the court also cited as one of its authorities the very quotation from the Supreme Court case 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*, *United States v. United States District Court*, *supra*, note 99, at 314. *Id.* at 407.

that courts strictly construe content-based restrictions and prior restraints to ensure they are narrowly tailored to advance a compelling government interest.”¹⁶⁸ The imposition of Congressional standards of court review rendered judicial review illusory, and violated the separation of powers clause.¹⁶⁹ The court held that Congress “may not legislatively supercede our decisions interpreting and applying the Constitution;” such an attempt “breaches the proper constitutional limits drawn for our government by the concepts of the separation and balance of power.”¹⁷⁰

One problem addressed by Doe I was not resolved by the Reauthorization Acts: an NSL asks for transactional records, without providing the recipient any guidance. The statute merely “directs the recipient to determine for itself whether any information it maintains regarding the target of the NSL” is responsive and whether the information is a “record” but not “content.”

¹⁷¹ So the response to an NSL could improperly reveal the dates and times the target accessed the internet, the contents of queries made to search engines, and histories of websites visited.¹⁷²

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, in violation of the

¹⁶⁸ *Id.* at 409.

¹⁶⁹ *Id.* at 411.

¹⁷⁰ *Id.*

¹⁷¹ *Id.* at 387.

¹⁷² *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.

Fourth Amendment requirement that a warrant be issued for content.¹⁷³ An NSL statute that allows the collection of content without a warrant is a statute in serious need of amendment.

After both the administrative and judicial investigation of the 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 execute subpoenas without sufficient judicial oversight is not a model destined to produce restraint.¹⁷⁴

¹⁷³ The warrant requirement for process directed to content is a basis tenet of Fourth Amendment law. *Smith v. Maryland*, 442 U.S. 735, 745-46 (1979). Although the plaintiffs in *Doe I* dropped their Fourth Amendment due process claims in light of the provision for judicial review added by the Reauthorization Acts (*Doe III* 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 the Application of the U.S. for an order Authorizing Use of Pen Register and Trap on (XXX) Internet Service Account/User Name*, 396 F.Supp.2d 45, 49-50 (D. Mass. 2005), where the court denied 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.. This case and other pen register cases are discussed more fully, *infra*, at .

¹⁷⁴ 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 “opposition to government policy or the expression of controversial views was frequently considered sufficient for collecting data on

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 national security letter provisions has a sunset provision.¹⁷⁵ The National Security Letter Reform Act requires that Section 2709 sunset December, 2009 and that it revert to its pre-Patriot Act language.¹⁷⁶ 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.¹⁷⁷ 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

Americans;” the Church Committee worried that “where 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.” Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities Report, S. Rep. No. 94-755, Book II, at 169, 177-78. (1976).

¹⁷⁵ S. 2088, 110th Cong (2007).

¹⁷⁶ *Id.*, sections 2 and 8. The two other bills about NSLs are 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 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.

¹⁷⁷ S. 2088, *supra*, note 175, at section 2.

statute.

Patriot Act Search Warrants

Search warrants have always been available to demand library records, computers, backup tapes, or any other tangible item.¹⁷⁸ Search warrants are immediately executable with or without the library's cooperation. 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 what is specified in the warrant is searched or taken.¹⁷⁹ 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.¹⁸⁰ 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 the *Tattered Cover* case, and the final result of granting that request for delay was the decision of the Colorado Supreme Court refusing to enforce the warrant for the bookstore's patron purchase records on both First and Fourth Amendment grounds.¹⁸¹

¹⁷⁸ A search warrant may be directed to a library for any information, patron specific or not, so long as the material has “evidential value.” *Patriot in the Library*, *supra*, note 9, at 377, citing *Warden v. Hayden*, 387 U.S. 294, 310 (1967).

¹⁷⁹ *Id.* at 384-85.

¹⁸⁰ *Id.* at 385.

¹⁸¹ *Tattered Cover, Inc.*, *supra*, note 8. The warrant was issued because the police found a mailer from the bookstore outside a meth lab, as well as two books on setting up drug labs; the police were trying to discover customer purchase records for the two books. *Id.* Long after the

Polite but persistent refusal to comply with a request unless legal process is issued may result in the demand disappearing, as happened to a Washington librarian, Joan Airoidi.¹⁸² An agent of the FBI 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.¹⁸³ The FBI then issued a subpoena¹⁸⁴ to try and find out who had written a quotation from a bin Laden speech in the margin of the book. The library board voted unanimously to go to court to quash the FBI subpoena, and fifteen days later, the FBI withdrew its request.¹⁸⁵ But it was a bittersweet victory for Ms. Airoidi, who knew the result would have been different if her library has received a Patriot Act order:

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 *Guide to Remembering Japanese Characters* by Kenneth G. Henshall. *Tattered Cover vs. U.S. Gov't: Denver Bookseller Leads Struggle Against Patriot Act Civil Liberties Violations*, DEMOCRACY NOW, http://www.democracynow.org/2004/5/6/tattered_cover_vs_u_s_govt, May 6, 2004.

¹⁸² Joan Airoidi, *Librarian's Brush With the FBI Shapes Her View of the Patriot Act*, USA Today.com, Jun. 17, 2005, http://www.usatoday.com/news/opinion/editorials/2005-05-17-librarian-edit_x.htm.

¹⁸³ *Id.*

¹⁸⁴ A subpoena is not issued by a court, so it is not technically "legal process." *A Patriot in the Library*, *supra*, note 9, at 379-80. It still cannot be ignored. *Id.*

¹⁸⁵ *Librarian's Brush With the FBI Shapes Her View of the Patriot Act*, *supra*, note 182.

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

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 issued the warrant on a showing of probable cause;¹⁸⁶ 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

¹⁸⁶ 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.'"

suppressed.¹⁸⁷ There is a higher standard for search warrants that are issued for library records, as the warrant implicates First Amendment rights.¹⁸⁸

The Patriot Act expanded the reach of search warrants by adding single jurisdiction search warrants, good nationwide.¹⁸⁹ This allows a search warrant issued in one jurisdiction to be served in any jurisdiction, for an indefinite period of time. The 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

¹⁸⁷ 3D FEDERAL PRACTICE & PROCEDURE – CRIMINAL, §677, *supra*, note 10: 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.”

¹⁸⁸ *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978).

¹⁸⁹ Patriot Act, § 219, 115 Stat. at 219, codified at FED. R. CRIM. P. 41: 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 country. Pursuant to the Patriot Act, § 220, 115 Stat. at 291-92, codified at 18 U.S.C. 2703 (Supp. I 2001), once the search warrant has been issued, it is valid nationwide.

place.¹⁹⁰ 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.¹⁹¹ The Patriot Act also broadened the types of electronic communications covered by search warrants.¹⁹²

¹⁹⁰ Patriot Act, § 213, 115 Stat. at 286-87, codified at 18 U.S.C.A. § 3103a (Supp. I 2001) (this section added 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."

¹⁹¹ Brian T. Yeh & Charles Doyle, USA PATRIOT Act Improvement and Reauthorization Act of 2005: A Legal Analysis, CRS Report for Congress, Dec. 21, 2006, at 24, Also available at <http://fas.org/sgp/crs/intel/RL33332.pdf>.

¹⁹² Patriot Act, § 209, Stat. at , codified at 18 U.S.C. 2510 and 2703 (Supp. I 2001). Although the title of Section 209 is “Seizure of Voice Mail Messages Pursuant to Warrant,” the actual changes in statutory language merely add the word ‘wire’ to the statutes. Several of the cases that have discussed search warrants as amended by the 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 (in Arizona) is the proper district, the court in *In re Search of Yahoo*, Slip Copy, 2007 WL 1539971 (D. Ariz. 2007), held, although all the records were held by Yahoo in California. The court cited with approval the unpublished case *In Re Search Warrant*, 19 Fla. L. Weekly Fed. D. 309 at 13, No. 6:05-MC-168-Orl-31JGG (M.D.Fla, Dec. 23, 2005), agreeing that Congress intended “jurisdiction” to mean territorial jurisdiction.

Reauthorization Act I Changed the Notice and Reporting Requirements for Search Warrants.

The Reauthorization Act I changed the delayed notification 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.¹⁹³ Additional extensions of time to give notice are limited to periods of ninety days.¹⁹⁴ 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 year.¹⁹⁵

Do the Delayed Notice Provisions Meet 4th Amendment Requirements?

Sneak and peek warrants allow surreptitious entry, and notice is not given until a “reasonable” period after the search. In one case analyzing a Patriot Act delayed notice search warrant, one district court thought that a **valid** delayed notice search was probably constitutional, since “the

¹⁹³ Reauthorization Act I, § 114, 120 Stat. at 210-11, to be codified at 18 U.S.C. 3103a (b), (c).

¹⁹⁴ *Id.*

¹⁹⁵ *Id.*, § 114(c), Stat. at , to be codified at 18 U.S.C. 3103a(d)(2). 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.

Supreme Court has ruled “the Fourth Amendment does not prohibit all surreptitious entries.”¹⁹⁶

The district court also noted the limits on surreptitious entries:

...the 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.¹⁹⁷

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.¹⁹⁸

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

¹⁹⁶ *U.S. v. Espinoza*, 2005 WL 3542519 (E.D.Wash., 2005), citing *United States v.*

Frietas, 800 F.2d 1451, 1456 (9th Cir.1986) (citing *Dalia v. United States*, 441 U.S. 238, (1979).

¹⁹⁷ *Id.*

¹⁹⁸ *Id.*

1, 2003, delayed notice warrants had been used 47 times.¹⁹⁹ Then requests for delayed notice warrants doubled in the period between April 2003 and January 2005 to 108, for a total of 155 requests.²⁰⁰ No request for delayed notice was ever denied.²⁰¹ Approximately 60 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.²⁰² Some targets of delayed notice search warrants have never been notified that they were the subjects of a clandestine search.²⁰³

The chart below summarizes the changes made by the Patriot Act and Reauthorization Act I:

¹⁹⁹ *Department of Justice Releases New Numbers on Section 213 of the Patriot Act*, http://www.usdoj.gov/opa/pr/2005/April/05_opa_160.htm; Oversight Hearing on the 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 H. Comm. on the Judiciary, Statement by Chairman Howard Coble, May 3, 2005.

²⁰⁰ *Id.*

²⁰¹ *Id.*

²⁰² USA Patriot Act, Hearing before the S. Select Comm. on Intelligence, 109th Cong. 341 (2005), Testimony on the USA Patriot Act by Bob Barr, at 6.

²⁰³ *Id.* at 7.

18 U.S.C. §§ 2510, 2703, 3103a; F.R. Crim. P. 41	Before the PATRIOT Act	After the 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. Contemporaneous 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 30 days; request for extension up to 90 days.	S. 2435 would limit the authority to delay notice to 7 days, and renewals to 21 days, and limits the causes for issuing a delayed notice, by removing “unduly delaying a trial” and “interfering with an investigation” from list of reasons might need delayed notice.
Sunset	No	No	No	S. 2435 would add this provision (Section 213) to the list of Patriot Act sections that would sunset in

18 U.S.C. §§ 2510, 2703, 3103a; F.R. Crim. P. 41	Before the PATRIOT Act	After the PATRIOT Act	After the Re-Authorization Act	Proposed Changes
				December 2009.

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.²⁰⁴ Because of these “catch-all” provisions, the potential for abuse of delayed notice search warrants cannot be ignored. Most delayed notice search warrants are in fact issued under the “catch-all” provisions.²⁰⁵ 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 Patriot Act to expire.²⁰⁶

²⁰⁴ 18 U.S.C. 2795(a)(2) (Supp. I 2001).

²⁰⁵ USA Patriot Act, Hearing Before the S. Select Comm. on Intelligence, *supra*, note 198.

²⁰⁶ S. 2435, 100th Cong. (2007).

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.²⁰⁷ To have a request for a wiretap order from the FISC approved, the applicant must show that there is **probable cause to believe the target is a foreign power or 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.²⁰⁸ And the government must certify that **a significant purpose of the surveillance is to gather foreign intelligence.**²⁰⁹ Prior to the passage of the Patriot Act, the government had to certify that **the** purpose of the surveillance was to gather foreign intelligence.²¹⁰ The Patriot Act also changed the scope of FISA wiretaps from district-wide to nationwide, and the wiretap can be attached to any computer the target of the order uses, including a library computer.²¹¹

²⁰⁷ 50 U.S.C. 1805(b)(2)(B) (Supp. I 2001).

²⁰⁸ 50 U.S.C. 1805(a) (Supp. I 2001).

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

²¹⁰ Patriot Act, § 218, amending 50 U.S.C. § 1823(a)(7)(B), 50 U.S.C. § 1804(a)(7)(B) (Supp. I 2001).

²¹¹ Patriot Act, § 206, 50 U.S.C. § 1805(b)(2)(B) (Supp. I 2001).

Some Interpretation of the Statutes

Only a few courts have directly addressed the constitutionality of the changes made by the 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.²¹² This decision was overruled in the first and only published decision of the FISA Court of Review, *In re Sealed Case*, which issued a decision on the scope of the "significant purpose" language.²¹³ 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**

²¹² *In re All Matters Submitted to Foreign Intelligence Surveillance Court*, 218

F.Supp.2d 611, 621-22 (Foreign Int. Surv. Ct. 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. Prior to the district court's decision, the government had violated the existing minimization procedures 75 times, by erroneously alleging a FISA target was not under criminal investigation, omission of material facts about the relationship between the FBI and a FISA target, and erroneous statements about meeting the minimization procedures. *Id.* at 620-21.

²¹³ 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002).

foreign intelligence purpose.²¹⁴

In *Mayfield v. U.S.*, the government used the FISC's process without any really good evidence that the target was an agent of a foreign power.²¹⁵ In March 2004, Brandon Mayfield was arrested as a suspect in the terrorist bombing in Madrid.²¹⁶ Mayfield was 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.²¹⁷ Although the evidence of a match 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.²¹⁸ These stories were leaked to the press.²¹⁹ Several weeks into Mayfield's detention, the Spanish authorities notified the

²¹⁴ *Id.* at 736-39. The Department of Justice 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 Senate Comm. on the Judiciary, 107th Cong. 20 (2002) (statement of Professor William C. Banks, Professor of Law, Syracuse University, Syracuse, New York), available at <http://www.access.gpo.gov/congress/senate/senate14ch107.html>.

²¹⁵ 504 F.Supp.2d 1023, 1026-29 (D.C. OR, 2007).

²¹⁶ *Id.*

²¹⁷ *Id.* at 1027.

²¹⁸ *Id.* at 1029.

²¹⁹ *Id.*

government that they had matched the fingerprint to an Algerian, and Mayfield was released.²²⁰

Mayfield filed suit, charging that the government's searches under FISA allowing circumvention of the Fourth Amendment's probable cause requirements violate the Constitution.

Mayfield's complaint directly attacked the "significant purpose" language added by the Patriot Act, alleging that the government can improperly avoid the strictures of the Fourth Amendment merely by "asserting a desire to also gather foreign intelligence from the person the government intends to criminally prosecute," so long as the government represents that the target was an agent of a foreign power, an assertion the court must accept unless clearly erroneous.²²¹ The court agreed, 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.²²²

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

²²⁰ *Id.*

²²¹ *Id.* at 1032-33.

²²² *Id.* at 1037.

Amendment – has no definitive jurisprudential answer.”²²³ 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 Patriot Act, and criminal investigators are free to seek Title III orders for criminal investigations whose definitions have been expanded to include virtually all terrorism and espionage-related offenses.²²⁴ 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 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 FISC 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.²²⁵

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

²²³ *Id.* at 1041.

²²⁴ *Id.*

²²⁵ *Id.* at 1042-43.

intelligence investigation in a trial for domestic crimes, focusing on the differing standards for probable cause for a Title III warrant and a FISA warrant. These defendants have not been so successful. In *U.S. v. Ning Wen*, 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.

²²⁶ 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 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.²²⁷

In *United States v. Damrah*, the defendant was found guilty of unlawfully obtaining citizenship by making false statements in a citizenship application and interview. 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.²²⁸ And a FISA warrant was upheld in

²²⁶ 477 F.3d 896, 897 (7th Cir. 2007).

²²⁷ *Id.* at 898-99.

²²⁸ 412 F.3d 618, 625 (6th Cir.2005). The court noted that "FISA has uniformly been held to be consistent with the Fourth Amendment," citing *In re Sealed Case* with approval. *Id.* Of course, *Mayfield* had not been decided yet. In several other cases, defendant's motions to suppress

U.S. v. Rosen, 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 and the court ruled that the allegations of the government that some of the defendants' lobbying activities were unlawful was sufficient to overcome the statutory bar on using FISA for activities protected by the First Amendment.²²⁹

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, as

have been denied, sometimes on procedural grounds, as in *U.S. v. Jayyousi*, 2007 WL 781373 (S.D.Fla.), 20 Fla. L. Weekly Fed. D 647 (2007) (rejecting claims that defendant's actions were protected by the First Amendment). In *U.S. v. Benkahla*, 437 F.Supp.2d 541 (E.D. Virginia 2006), the court rejected the defendant's claim that his computer was illegally seized; the court only analyzed pre-Patriot act case law as no other authority had been provided. In *U.S. v. Holy Land Foundation for Relief and Development*, Slip Copy, 2007 WL 2011319 (N.D. Tex), 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, *supra*, and held that FISA did not violate the Fourth Amendment. In *U.S. v. Marzook*, 35 F.Supp. 2d 778, 779-80, 792-94 (N.D. Ill. 2006), the court was faced with a pre-Patriot Act FISA warrant for a physical search, and held that the search was reasonable and was authorized for "foreign intelligence."

²²⁹ 447 F.Supp.2d 538, 549-51 (E.D. Vir. 2006).

in *Mayfield*, the court found FISA did not comport with the Fourth Amendment. But where the facts were 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 and to deny any motions to suppress.

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."²³⁰ The Reauthorization Act I expanded the list of predicate offenses to 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.²³¹

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

²³⁰ 18 U.S.C. 2616(1) (2000).

²³¹ Brian T. Yeh & Charles Doyle, USA PATRIOT Act Improvement and Reauthorization Act of 2005: A Legal Analysis, CRS Report for Congress, Dec. 21, 2006, at 24, Also available at <http://fas.org/sgp/crs/intel/RL33332.pdf>.

roving wiretap.²³² 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.²³³ And a description of the total number of applications for roving wiretaps made each year now has to be reported to Congressional committees.²³⁴ The Reauthorization Act I extends the date for the section of the Patriot Act authorizing roving wiretaps to expire until December 31, 2009.²³⁵

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 in 2005, another increase over the previous year.²³⁶ Only one application was denied by the courts.²³⁷ In 2004 state and federal courts authorized

²³² Reauthorization Act I, § 108, 120 Stat. at 203-04, to be codified at 50 U.S.C.

1804(a)(3) and 50 U.S.C. 1805(c)(1)(A).

²³³ *Id.*, § 108 (b)(4), to be codified at 50 U.S.C. 1805(c)(3).

²³⁴ *Id.*, § 108 (c)(2), to be codified at 50 U.S.C. 1808 (a)(2).

²³⁵ *Id.*, § 102(b), 120 Stat. at 194-95.

²³⁶ 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, http://epic.org/privacy/wiretap/2005_wiretap_report.pdf, May 2, 2006, at 5. The report does not include FISA orders.

²³⁷ *Id.*

1,710 interceptions of wire, oral, and electronic communications.²³⁸ This was an increase of 19 percent over intercepts approved in 2003 and the greatest number ever authorized in a single year.²³⁹ Federal officials requested 730 intercept applications in 2004, a 26 percent increase over the number requested in 2003.²⁴⁰ No wiretap applications were denied.²⁴¹ In 2003, there were 1,442 interceptions of wire, oral and electronic communications, an increase of 6 percent over interceptions authorized in 2002.²⁴² The agency also reported that federal officials requested 578 intercept applications in 2003, a 16 percent increase over those requested in 2002.²⁴³ No wiretap applications were denied.²⁴⁴ These statistics do not include FISA roving wiretaps; such information as is available on FISA roving wiretaps is included in a letter report

²³⁸ 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, Apr. 2005, <http://www.uscourts.gov/wiretap04/2004WireTap.pdf>, at 5.

²³⁹ *Id.*

²⁴⁰ *Id.*

²⁴¹ *Id.*

²⁴² 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, Apr. 2004, <http://www.uscourts.gov/wiretap03/2003WireTap.pdf>.

²⁴³ *Id.*

²⁴⁴ *Id.*

the Attorney General makes to Congress, showing that applications for FISA surveillance orders have also increased over the reported years, and that applications are not denied.²⁴⁵

The chart below describes the changes made to the roving wiretap laws by the Patriot Act and the Reauthorization Act I.

50 U.S.C. §§ 1804, 1805	Before the PATRIOT Act	After the 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 the agent of a foreign power. No U.S. person may be considered	The same certification, but with nation-wide, not district-wide, effect.	Applications for orders, as well as orders, have to identify the <i>specific</i> target of the electronic surveillance if the target's identity is not known; must state specific

²⁴⁵ U.S. Department of Justice, Office of Legislative Affairs, Office of the Assistant Attorney General, letter to J. Dennis Hastert, Apr. 28, 2006, <http://www.fas.org/irp/agency/doj/fisa/2005rept.html>; U.S. Department of Justice, Office of Legislative Affairs, Office of the Assistant Attorney General, letter to J. Dennis Hastert, Apr. 1, 2005, <http://www.fas.org/irp/agency/doj/fisa/2004rept.pdf>; see notes 257 and 288, *infra*, and related text.

50 U.S.C. §§ 1804, 1805	Before the PATRIOT Act	After the PATRIOT Act	After the Re-Authorization Act
	a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Co		facts that lead to conclusion target will thwart ; new locations must be disclosed to the court within 10 days
Gag Order & Disclosure	Yes, must comply with order and “accomplish the electronic surveillance in such a manner as will protect its secrecy (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

Section 216 & Section 214 Pen Register/Trap & Trace Orders

The Patriot Act expanded the scope of pen register/trap & trace orders²⁴⁶ in national security

²⁴⁶ A pen register is "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses cause when the dial on the telephone is released," 442 U.S. 735, 736 n.1 (1979). The trap and trace device is the reverse of a pen register; it records incoming information. 18 U.S.C. § 3127(4) (Supp. 2001). Both will be referred to as “pen

cases. There are two types of pen register orders that were changed by the 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 noncontent information from computers, not just from telephones.²⁴⁷ Section 214 gave the FISC the same expanded authority.²⁴⁸ 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-

registers.” Because recording incoming and outgoing telephone numbers was not considered a “search” requiring a warrant under *Smith v. Maryland*, 442 U.S. 735, 745-46 (1979), 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 (1986) (codified at 18 U.S.C. § 3123(a) (2000)).

²⁴⁷ Patriot Act, 115 Stat. at 288-90, amending 18 U.S.C. §§ 3121 (c), 3123 (a), 3123(b)(1), 3123(d)(2), 3124(b), 3124(d), 3127(1)-(4) (Supp. I 2001) For a more detailed discussion of the changes made to Section 216 by the Patriot Act., see Susan Nevelow Mart, *Protecting the Lady From Toledo*, 96-L. LIBR. J.449, 452-53 (2004).

²⁴⁸ Patriot Act, § 214, 115 Stat. at 286-87, codified at 50 U.S.C. § 1842 (Supp. I 2001).

cut-through dialed digit extraction.²⁴⁹ IP addresses also can reveal content. In *Mass. Pen Register Application*, the court was troubled by the government’s application for:

Internet Protocol (IP) addresses which are defined as a “unique numerical address identifying each computer on the internet.” The internet service provider 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... 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...²⁵⁰

The court was concerned that Internet Service Providers (ISP) 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 contempt of court penalties on the ISP for failure to comply.²⁵¹ The court hoped that

²⁴⁹ *In re Application of U.S. for an Order Authorizing Use Of A Pen Register and Trap on (XXX) Internet Service Account/User Name (xxxxxxx@xxx.com)*, 396 F.Supp.2d 45, 48 (D. Mass. 2005).[*Mass. Pen Register Application*]. See also, *In Matter of 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.

²⁵⁰ *Mass. Pen Register Application*, *supra*, note 249 at 48-49.

²⁵¹ *Id.* at 49.

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.²⁵²

In the case of telephone numbers, technology is not currently up to the challenge. In a case from the Southern District in 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 from those that may constitute content."²⁵³

The court rejected the government's pledge that it would make no affirmative use of content digits, and held that the Patriot Act amendments require more than overcollection 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.²⁵⁴

²⁵² See the cases discussed in note 249, *supra*.

²⁵³ 441 F.Supp.2d 816, 822-23, (S.D. Tex. (2006). See also *In re U.S. for Orders (1) Authorizing Use of Pen Registers*, 515 F.Supp.2d 325 (E.D.N.Y. 2007) (government's position that pen/trap statute authorized access to all dialed digits violated Fourth Amendment); *In re U.S.*, U.S. Dist. LEXIS 77635, WL 3036849 (S.D. Tex. 2007) (refusing to issue a pen register order for post-cut-through dialed digits)

²⁵⁴ *Id.* at 825-26.

The Sixth Circuit has expressly ruled on the limit of process to collect 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.²⁵⁵

Section 214 pen register orders are issued by the FISC,²⁵⁶ but otherwise the post-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.²⁵⁷

²⁵⁵ *Warshak v. U.S.*, 490 F.3d 455, 470-476 (6th Cir. 2007); analysis followed by *In re U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government* (___F.Supp.2d ___ (W.D. Penn. 2008), 2008 WL 48343) to deny the government's request for cell phone subscriber information for use in identifying the user's past or present physical/geographical location..

²⁵⁶ Patriot Act, § 214, 115 Stat. at 286-87, amending 50 U.S.C. § 1842 (2000).

²⁵⁷ Patriot Act, § 216(b)(1), 115 Stat. at 288-90, codified at 18 U.S.C. 3123(a) (Supp. I 2001). The software developed by the government was known as Carnivore, and is now known as DCS 1000. Nomination of Robert S. Mueller, III to be Director of the Federal Bureau of Investigation: Hearing Before the Senate Comm. on the Judiciary, 107th Cong. 108 (2001) (statement of Robert S. Mueller).

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.²⁵⁸ 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 extension of an order, under this section may be for a period not to exceed one year.”²⁵⁹

²⁵⁸ Reauthorization Act I, § 128, 120 Stat. at 228-29, to be codified at 50 U.S.C.1842(d)(20)(C).

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.* This makes the pen register closer to a national security letter. *See* S. Report 109-58 (2005), at 8.

²⁵⁹ Reauthorization Act I, § 105, 120 Stat. at 195-96, to be codified at 50 U.S.C. 1842(e)(2).

Reauthorization Act I also requires additional reporting: the Judiciary Committee must receive full reports on the use of pen registers/trap & trace devices every six months.²⁶⁰

Some Statistics on the Use of FISA Court Process

The information that is available about the FISC is not very specific. In 2005, the government made 2,074 applications to the Foreign Intelligence Surveillance Court (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.²⁶¹ In 2004, the government made 1,758 applications to the Foreign Intelligence Surveillance Court (FISC) for authority to conduct electronic surveillance and physical search for foreign intelligence purposes, and none were denied.²⁶²

The changes made to Section 214 pen registers are summarized in the chart below:

²⁶⁰ Reauthorization Act I, §128(b), to be codified at 50 U.S.C. 1846(a).

²⁶¹ U.S. Department of Justice, Office of Legislative Affairs, Office of the Assistant Attorney General, letter to J. Dennis Hastert, Apr. 28, 2006, <http://www.fas.org/irp/agency/doj/fisa/2005rept.html>. The FISC made substantive modifications to the Government's proposed orders in 61 of those applications. *Id.* The FISC did not deny, in whole or in part, any application filed by the Government during calendar year 2005. *Id.*

²⁶² U.S. Department of Justice, Office of Legislative Affairs, Office of the Assistant Attorney General, letter to J. Dennis Hastert, Apr. 1, 2005, <http://www.fas.org/irp/agency/doj/fisa/2004rept.pdf>.

50 U.S.C. §§ 1842	Before the PATRIOT Act	After the PATRIOT Act	After the Re-Authorization Act
Records and Duration	Telephone numbers dialed within a specific federal district.	Real-time interception of “noncontent” information from computers, as well as telephones. All orders are roving orders, and are good for 90 days.	Initial orders for non-U.S. persons can be requested or renewed for as long as 1 year (Section 105). Courts may authorize release of customer information in addition to dialing or IP information.
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. Any district court can issue the order.	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 60 days, with renewals (no specific penalty/contempt of court)	The same	The same
Review of the Order	Yes	The same	The same
Library Section	No	No	No
Sunset	N/A	No	No

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 datamining efforts,²⁶³ one must ask if there has been any significant benefit to the cause of preventing terrorism that has resulted since the implementation of the Patriot Act. The balance between the preservation of civil liberties and the prevention of terrorism has always been the crux of the problem, whether you believe that the government has been overzealous in its efforts to prevent terrorism at the expense of civil liberties or 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 Patriot Act should be instructive.

²⁶³ Although a discussion of all 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, Symposium On Electronic Privacy In The Information Age*, 41 Val. U. L. Rev. 1481(2007); Andrew P. MacArthur, *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. of Comp. & Int'l L. 441 (2007); and Steven W. Dummer, Note, *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).

The DOJ just published *Terrorism 2002-2005* 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.”²⁶⁴ From September 12, 2001 through 2005, the DOJ lists 27 incidents of terrorist attacks in the United States. Twenty-two of those incidents were perpetrated by the Earth Liberation Front or the Animal Liberation Front and involved crimes against property. The remaining five incidents are:

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

The Terrorism Report concluded that the longstanding trend is **that domestic extremists carry out the majority of terrorist incidents in the United States.**²⁶⁵

²⁶⁴ U.S. Department of Justice, Federal Bureau of Investigation, *TERRORISM 2002-2005*, http://www.fbi.gov/publications/terror/terrorism2002_2005.pdf, at iii [Terrorism Report]. The Terrorism Report also includes major FBI investigations overseas and identifies significant prosecutorial updates, legislative actions, and program developments relevant to counter-terrorism efforts.

²⁶⁵ The Terrorism Report, *supra*, note 264, at 29. (emphasis added).

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,”²⁶⁶ the Terrorism Report has this to say:

The terrorist preventions for 2002 through 2005 paint a more diverse threat picture. Eight of the 14 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.**²⁶⁷ (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 three 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.”²⁶⁸

²⁶⁶ *Id.* at v.

²⁶⁷ *Id.* at 29.

²⁶⁸ The Terrorism Report, *supra*, note X, at 25. See also Guy Lawson, *The Fear Factory*, ROLLING STONE, Feb. 7, 2008, for a story on the Joint Terrorism Task Force and some

So the apparatus of the war on terror has been directed at animal rights activists, homegrown right wing types, three 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 Patriot Act contributed to these preventions. Although we know that the use of Section 215 orders has not contributed to a prevention,²⁶⁹ other 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”²⁷⁰ And the 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

overblown claims of terrorist cells. The Rolling Stone also has an online list of all 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 that 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* ,

http://www.rollingstone.com/politics/story/18056504/truth_or_terrorism_the_real_story_behind_five_years_of_high_alerts, Feb. 7, 2008

²⁶⁹ Section 215 Audit Report, *supra*, note 65?, at 79.

²⁷⁰ Office of the Inspector General, Semiannual Report to Congress, April 1, 2007-September 2007, <http://www.usdoj.gov/oig/semiannual/0711/challenges.htm>, *supra*, note ?

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.”²⁷¹

²⁷¹ *Supra*, note 1.