National Security Letters: Unconstitutional Demands by U.S. Government

Copyright 2007 by Ronald B. Standler
no claim of copyright for text quoted from works of the U.S. government

Keywords

administrative subpoena, cases, First Amendment, Fourth Amendment, history, National Security Letter, NSL, NSLs, privacy, quotations, subpena, subpoena, subpoenas, unlawful, unconstitutional, 18 U.S.C. 2709

Table of Contents

Introduction 2

First Amendment 3

Fourth Amendment 3

Administrative Subpoenas 3

pre-PATRIOT Act versions of 18 U.S.C. § 2709 6
- 1993 amendments 7
- PATRIOT Act 10

Statutes in Sep 2007 10
- 18 U.S.C. § 2709 11
- 18 U.S.C. § 3511 13
- 18 U.S.C. § 1510 15

Court Cases on NSLs 16

Newspaper Articles on NSLs 17
- 24 March 2003 17
- 6 Nov 2005 18
- 9 March 2007 20
- 9 Sep 2007 22

Conclusion 24

Bibliography 24

Introduction

Astoundingly, federal statutes allow a government bureaucrat — without any judicial approval — issue a "National Security Letter" (NSL) that demands that the recipient provide the government with business records. According to the FBI's Inspector General, in the year 2004, the FBI issued 56,507 NSLs, of which approximately 29,000 involved U.S. persons.
As explained in this essay, NSLs under 18 U.S.C. § 2709 are *un*constitutional for several possible reasons:

1. NSLs may violate the Fourth Amendment to the U.S. Constitution by demanding evidence of individual U.S. citizen's behavior without a showing of probable cause and without a warrant issued by a neutral judge. As such, NSLs improperly allow the government to intrude into private conduct, such as demanding information about a U.S. citizen's communications.[1]

2. NSLs violate the First Amendment to the U.S. Constitution by demanding secrecy (i.e., "prior restraint") from the recipient, who is under a gag order to tell no one (except his/her attorney) about the NSL.[2]

3. The gag order prohibits the recipient from obtaining judicial review of the reasonableness of the NSL, which is one of the legal requirements for the validity of administrative subpoenas.[3]

4. The gag order violates the First Amendment right "to petition the Government for a redress of grievances."

5. Alternatively, having an employee of the executive branch issue an NSL without any judicial review or approval may violate separation of powers in the U.S. Constitution.

This essay presents the history of the use of NSLs and the history of how courts regulated the use of NSLs. This essay concentrates on 18 U.S.C. § 2709, one of five statutes giving government agents the power to issue National Security Letters.

This essay presents general information about an interesting topic in law, but is *not* legal advice for your specific problem. See my disclaimer at http://www.rbs2.com/disclaim.htm .

---

[1] Communications implicate constitutional rights to freedom of speech (including the right to anonymous speech) and freedom of association. See *Doe v. Ashcroft,* 334 F.Supp.2d 471, 506-511 (S.D.N.Y. 2004).

[2] *Doe v. Ashcroft,* 334 F.Supp.2d 471, 511-512 (S.D.N.Y. 2004); *Doe v. Gonzales,* 386 F.Supp.2d 66, 74 (D.Conn. 2005).

[3] *Doe v. Ashcroft,* 334 F.Supp.2d 471, 496-506 (S.D.N.Y. 2004).

I list the cases in chronological order in this essay, so the reader can easily follow the historical development of a national phenomenon. If I were writing a legal brief, then I would use the conventional citation order given in the *Bluebook*.

First Amendment

The First Amendment to the U.S. Constitution, as interpreted in numerous U.S. Supreme Court cases, prohibits the government from forbidding publication or other disclosure of information. For citations to U.S. Supreme Court cases, see my separate essay, *U.S. Government Restrictions on Scientific Publications,* at http://www.rbs2.com/OFAC.pdf in the sub-section titled " 'prior restraint' disfavored in USA".

Fourth Amendment

The Fourth Amendment to the U.S. Constitution requires the government to appear before a neutral, detached judge and obtain a search warrant *before* entering a person's home or business, for the purpose of either to search for things, to inspect, or to install a wiretap.[4] However, in an administrative subpoena, the government does not enter private property to make a search/inspection, instead the government demands that the recipient of the subpoena deliver documents to the government.[5]

Administrative Subpoenas

Various agencies of the executive branch of government (e.g., Securities and Exchange Commission,[6] Federal Trade Commission, Equal Employment Opportunity Commission, etc.) are authorized to issue subpoenas to corporations[7] to assist in their investigations.

---

[4] For citation to U.S. Supreme Court cases, see my essay on the *Foreign Intelligence Surveillance Act,* at http://www.rbs0.com/FISA.pdf , in the sub-section titled "Requirements in Ordinary Criminal Law".

[5] See, e.g., *Donovan v. Lone Steer, Inc.,* 464 U.S. 408, 413-415 (1984); *In re Subpoena Duces Tecum,* 228 F.3d 341, 347-349 (4thCir. 2000).

[6] 15 U.S.C. §§ 77t(c), 78u(b); *Penfield Co. of Cal. v. Securities and Exchange Commission,* 330 U.S. 585 (1947).

[7] While the statutes authorizing administrative subpoenas are not limited to corporate recipients, the nature of each government agency is to regulate corporations, *not* private individuals, so it is anticipated that the subpoenas will mostly be directed to corporations.

In 1967, the U.S. Supreme Court held:

> It is now settled that, when an administrative agency subpoenas corporate books or records, the Fourth Amendment requires that the subpoena be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.[FN5] The agency has the right to conduct all reasonable inspections of such documents which are contemplated by statute, but it must delimit the confines of a search by designating the needed documents in a formal subpoena. In addition, while the demand to inspect may be issued by the agency, in the form of an administrative subpoena, it may not be made and enforced by the inspector in the field, and the subpoenaed party may obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply.
>
> FN5. See *United States v. Morton Salt Co.,* 338 U.S. 632, 70 S.Ct. 357, 94 L.Ed. 40; *Oklahoma Press Pub. Co. v. Walling,* 327 U.S. 186, 66 S.Ct. 494, 90 L.Ed. 614, 166 A.L.R. 531; *United States v. Bausch & Lomb Optical Co.,* 321 U.S. 707, 64 S.Ct. 805, 88 L.Ed. 1024; *Hale v. Henkel,* 201 U.S. 43, 26 S.Ct. 370, 50 L.Ed. 652. See generally 1 Davis, ADMINISTRATIVE LAW §§ 3.05-3.06 (1958).

See v. City of Seattle, 387 U.S. 541, 544-545 (1967).

Judge Marrero, in a U.S. District Court case involving a National Security Letter, discussed the law for administrative subpoenas, such as National Security Letters:

> However, because administrative subpoenas are "at best, constructive searches," there is no requirement that they be issued pursuant to a warrant or that they be supported by probable cause. [footnote omitted] Instead, an administrative subpoena needs only to be "reasonable," which the Supreme Court has interpreted to mean that (1) the administrative subpoena is "within the authority of the agency;" (2) that the demand is "not too indefinite;" and (3) that the information sought is "reasonably relevant" to a proper inquiry. [FN124]
>
> While the Fourth Amendment reasonableness standard is permissive in the context of administrative subpoenas, the constitutionality of the administrative subpoena is predicated on the availability of a neutral tribunal to determine, after a subpoena is issued, whether the subpoena actually complies with the Fourth Amendment's demands. In contrast to an actual physical search, which must be justified by the warrant and probable cause requirements occurring before the search, an administrative subpoena "is regulated by, and its justification derives from, [judicial] process" available after the subpoena is issued. [footnote omitted]
>
> Accordingly, the Supreme Court has held that an administrative subpoena "may not be made and enforced" by the administrative agency; rather, the subpoenaed party must be able to "obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply." [FN126] In sum, longstanding Supreme Court doctrine makes clear that an administrative subpoena statute is consistent with the Fourth Amendment when it is subject to "judicial supervision" and "surrounded by every safeguard of judicial restraint." [FN127]
>
> FN124 *Morton Salt Co.,* 338 U.S. at 652, 70 S.Ct. 357 [(1950)]; see also *Oklahoma Press Pub. Co. v. Walling,* 327 U.S. 186, 208, 66 S.Ct. 494, 90 L.Ed. 614 (1946) ("The gist of the protection is ... that the disclosure sought shall not be unreasonable.").
>
> FN126. *See v. City of Seattle,* 387 U.S. 541, 544-45, 87 S.Ct. 1737, 18 L.Ed.2d 943 (1967); see also *Oklahoma Press,* 327 U.S. at 217, 66 S.Ct. 494

FN127. *Oklahoma Press,* 327 U.S. at 217, 66 S.Ct. 494.
Doe v. Ashcroft, 334 F.Supp.2d 471, 495 (S.D.N.Y. 2004),
rev'd on grounds of mootness, 449 F.3d 415 (2nd Cir. 23 May 2006).

A U.S. Court of Appeals wrote in the year 1982 about the distinction between issuing and enforcing administrative subpoenas:

> At least since *ICC v. Brimson,* 154 U.S. 447, 485, 14 S.Ct. 1125, 1136, 38 L.Ed. 1047 (1894), federal courts have drawn a sharp distinction between agency power to *issue* subpoenas and judicial power to *enforce* them. E.g., *United States v. Exxon Corp.,* 628 F.2d 70, 77 (D.C.Cir. [1980]) (per curiam), *cert. denied,* 446 U.S. 964, 100 S.Ct. 2940, 64 L.Ed.2d 823 (1980); *United States v. Bell,* 564 F.2d 953, 959 (Em.App. 1977); see L. Jaffe, JUDICIAL CONTROL OF ADMINISTRATIVE ACTION 115-17 (1965). [FN15]
>
> FN15. This "[b]ifurcation of the power, on the one hand of the agency to issue subpoenas and on the other hand of the courts to enforce them, is an inherent protection against abuse of subpoena power." *United States v. Bell,* 564 F.2d at 959; accord *United States v. Security State Bank & Trust,* 473 F.2d 638, 641 (5th Cir. 1973); F. Cooper, ADMINISTRATIVE AGENCIES AND THE COURTS 129-31 (1951).

U.S. v. Hill, 694 F.2d 258, 263 (C.A.D.C. 1982).

Most administrative subpoenas are directed at a corporation for disclosure of corporate business records. It is well established that individual citizens have privacy rights, but corporations have no privacy rights,[8] so subpoenas (or National Security Letters) directed at a corporation for disclosure of information about the health or communications[9] of individual citizens raises legal issues not found in typical administrative subpoena cases involving behavior of corporations. For this reason, I suggest that the administrative subpoena precedents are distinguishable from the issues in National Security Letter cases involving demands for private information about individuals.

---

[8] See, e.g., *Oklahoma Press Pub. Co. v. Walling,* 327 U.S. 186, 205-206 (1946); *U.S. v. Morton Salt Co.,* 338 U.S. 632, 651-652 (1950); *California Bankers Ass'n v. Shultz,* 416 U.S. 21, 65 (1974) ("... corporations can claim no equality with individuals in the enjoyment of a right to privacy."); *First Nat. Bank of Boston v. Bellotti,* 435 U.S. 765, 778, n. 14 (1978).

[9] Communications of individual citizens are protected by freedom of speech in the First Amendment of the U.S. Constitution.

pre-PATRIOT Act versions of 18 U.S.C. § 2709

There are now five federal statutes that give government agents the authority to issue what are now known as National Security Letters. According to Doyle,[10] the first of these statutes was enacted in 1978.

The original Electronic Communications Privacy Act of 1986 (ECPA) contained one section, 18 U.S.C. § 2709, that is one of the early statutory occurrences of National Security Letters.

> (a) DUTY TO PROVIDE. — A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.
>
> (b) REQUIRED CERTIFICATION. — The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the wire or electronic communication service provider to which the request is made that —
>
> (1) **the information sought is relevant to an authorized foreign counterintelligence investigation**;[11] and
>
> (2) there are **specific and articulable facts**[12] 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 as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801).
>
> (c) PROHIBITION OF CERTAIN DISCLOSURE. — No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.
>
> (d) DISSEMINATION BY BUREAU. — The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

---

[10] Charles Doyle, National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments, Congressional Research Service, p. 2 (20 March 2007).

[11] Boldface added by Standler.

[12] Boldface added by Standler.

> (e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED. — On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

18 U.S.C. § 2709 (as enacted 1986).

Subsection (c) is blatantly *un*constitutional. It is an example of prior restraint of speech, which is a violation of the First Amendment to the U.S. Constitution. It is a violation of another part of the First Amendment: the right "to petition the Government for a redress of grievances." Furthermore, by prohibiting litigation in a public court over the request, this statute violates a condition for lawful administrative subpoenas. It's ironic that a so-called "Privacy Act" contains such an assault on privacy of people in the USA. Still further, this statute may violate the Fifth Amendment, in that the government does *not* reimburse the recipient of the subpoena for the cost of complying with that subpoena.[13]

There are three additional problems with § 2709 as originally enacted in 1986: the statute (1) lacked any judicial enforcement of the NSL, (2) lacked any provision for the recipient to challenge the NSL in court, and (3) lacked any penalties for violation of the gag order in § 2709(c). These three defects were first repaired when the statute was amended in the year 2006, twenty years after the statute was first enacted. These defects were *not* difficult to repair. Since the early 1940s there were numerous federal statutes that gave a government agency the ability to issue an administrative subpoena, have a court compel compliance with the subpoena under the court's contempt power, and permit the recipient to challenge the subpoena in court. When drafting the ECPA in 1986, Congress could have simply copied any of these earlier statutes, which had already been interpreted and validated by federal courts.

1993 amendments

In 1993, subsection (b) was amended by Congress. The U.S. House of Representatives issued a report that contains the legislative history of this amendment:

BACKGROUND

> In adopting ECPA in 1986, Congress established certain privacy protections for subscriber records and other information held by telephone companies and other electronic communication service providers. Congress provided that the government could obtain a subscriber's transactional records or other information from a telephone company without the subscriber's permission only pursuant to a subpoena, search warrant or court order where

---

[13] Two of the five federal statutes permitting issuance of National Security Letters specifically authorize the government to reimburse expenses of searching and reproducing records. 15 U.S.C. § 1681u (e) (Fair Credit Reporting Act, enacted 1968) and 50 U.S.C. § 436 (d).

there is reason to believe that the information is relevant to a legitimate law enforcement inquiry. 18 U.S.C. § 2703.

Congress created a limited exception to this rule for use in counterintelligence and international terrorism cases. In 18 U.S.C. § 2709, Congress gave the FBI authority to compel production of identifying information and toll records with a so-called "national security letter," signed by an FBI official without judicial review and without relevance to a criminal investigation, where the subscriber is believed to be a foreign power or agent of a foreign power, as defined in the Foreign Intelligence Surveillance Act. ("Foreign power" includes international terrorist groups.)

The FBI has concluded that the authority in § 2709 is, in one specific respect, too narrow. To illustrate the problem, the Bureau cites the case of a former employee of the U.S. government who called a foreign embassy and offered to provide sensitive U.S. government information. The conversation was monitored, but the former employee did not identify himself. The former employee subsequently met with representatives of the foreign nation and compromised highly sensitive information about U.S. intelligence capabilities. The FBI argues that if it had been able to trace the number from which the first call offering information was placed, it might have been able to identify the former employee sooner or prevent the loss of information.

However, under §§ 2703 and 2709 as they were adopted in 1986, the FBI could not, without a subpoena or court order, obtain the identity of a subscriber, unless there was a reason to believe that the subscriber was a foreign power or agent of a foreign power. In the case described above, the FBI did not have reason to believe that the caller was a foreign agent. Instead, the caller appeared to be a possible volunteer to be an agent, and therefore did not meet the § 2709 standard.

In response to this limitation, the FBI asked Congress to expand the reach of § 2709, to allow the FBI certification to require phone companies to identify not only suspected agents of foreign powers but also persons who have been in contact with foreign powers or suspected agents of foreign powers. As originally proposed by the FBI, the amendment would have applied to any caller to a foreign diplomatic establishment and any caller to official foreign visitors such as scholars from government universities abroad. This was deemed by the Committee to be too broad.

Exempt from the judicial scrutiny normally required for compulsory process, the national security letter is an extraordinary device. New applications are disfavored.[14] However, after careful study, the Committee concluded that a narrow change in § 2709 to meet the FBI's focused and demonstrated needs was justified. H.R. 175 as reported by the Committee is a modification of the language originally proposed by the FBI. It allows access where: (1) there is a contact with a suspected intelligence officer or a suspected terrorist, or (2) the circumstances of the conversation indicate, as they did in the case described above, that it may involve spying or an offer of information.

In addition to covering a future case like the one described above, this new authority would allow the FBI to identify subscribers in the following types of cases, cited by the FBI in justifying its need for this amendment:

(1) Persons whose phone numbers were listed in an address book seized from a suspected terrorist;
(2) All persons who call an embassy and ask to speak with a suspected intelligence officer; and

---

[14] Boldface added by Standler.

(3) All callers to the home of a suspected intelligence officer or the apartment of a suspected terrorist.

....

U.S. House of Representatives Report 103-46 (29 March 1993), reprinted in 1993 U.S. CODE CONGRESSIONAL AND ADMINISTRATIVE NEWS 1914-1915.

With the 1993 changes, 18 U.S.C. § 2709(b) became:

(b) REQUIRED CERTIFICATION. — The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director, may —

(1) request the name, address, length of service, and *local and long distance*[15] toll billing records of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that —

(A) the name, address, length of service, and toll billing records sought are relevant to an authorized foreign counterintelligence investigation; and

(B) there are 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 as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801); and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that --

(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with —

(i) an individual who is engaging or has engaged in international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or

(ii) a foreign power or an agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States.

18 U.S.C. § 2709 (17 Nov 1993, and amended in 1996), 107 Stat. 1491-92, 110 Stat. 3469.

---

[15] Phrase in italics inserted in 11 Oct 1996 amendment. 110 Stat. 3469.

PATRIOT Act

In October 2001, the U.S. Congress hastily passed the PATRIOT Act[16] which — among many other provisions — contained modifications to 18 U.S.C. § 2709. Neither the House of Representatives nor the Senate issued a report on the PATRIOT Act, so the only legislative history is what appears in speeches on the floor that are published in the CONGRESSIONAL RECORD. The following is a list of the three most significant changes to § 2709 made by the USA PATRIOT Act of 2001, § 505:

- The 1986 version of § 2709(b)(2) required "there are 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 as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801)." The PATRIOT Act broadened this requirement: "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." Note that the PATRIOT Act deleted the requirement for "specific and articulable facts" to support the NSL, which made it easier for the FBI to issue NSLs. Note that the PATRIOT Act deleted the nexus to "foreign power", as defined in FISA.

- The 1986 and 1993 versions of § 2709 required approval from a high-level officer ("not lower than Deputy Assistant Director") at FBI headquarters for each NSL. The USA PATRIOT Act of 2001, allowed the Special Agent in Charge of a field office to approve NSLs, making it much easier to issue NSLs.

Statutes in Sep 2007

In the House of Representatives Conference Report 109-333 for the "USA PATRIOT Improvement and Reauthorization Act of 2005" there appears a definition of *National Security Letters*. This definition was apparently intended to be inserted in the U.S. Code at 15 U.S. § 1681v, but my search of the U.S. Code on 12 Sep 2007 did *not* find the following definition anywhere in the U.S. Code:

> (d) National Security Letter Defined — In this section, the term "national security letter" means a request for information under one of the following provisions of law:
>
> (1) Section 2709(a) of title 18, United States Code (to access certain communication service provider records).
>
> (2) Section 1114(a)(5)(A) of the Right to Financial Privacy Act (12 U.S.C. § 3414(a)(5)(A)) (to obtain financial institution customer records).

[16] See my essay at http://www.rbs0.com/patriot.pdf for a history of the PATRIOT Act.

(3) Section 802 of the National Security Act of 1947 (50 U.S.C. § 436) (to obtain financial information, records, and consumer reports).

(4) Section 626 of the Fair Credit Reporting Act (15 U.S.C. § 1681u) (to obtain certain financial information and consumer reports).

(5) Section 627 of the Fair Credit Reporting Act (15 U.S.C. § 1681v) (to obtain credit agency consumer records for counterterrorism investigations).

House of Representatives Conference Report 109-333, USA PATRIOT Improvement and Reauthorization Act of 2005 (8 Dec 2005). This text became Public Law Nr. 109-177, § 118, 120 Stat. 218 (9 March 2006).

The same definition also appears in the USA PATRIOT Improvement and Reauthorization Act of 2005, Public Law Nr. 109-177 at § 119, 120 Stat. 220-221 (9 March 2006).

18 U.S.C. § 2709
part of The Electronic Communications Privacy Act

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) Duty to provide. — A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification. — The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or **a Special Agent in Charge in a Bureau field office**[17] designated by the Director, may —
(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are **relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities**,[18] provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

---

[17] Boldface added by Standler. This is a significant change from the 1986 and 1993 versions.

[18] Boldface added by Standler. This is a significant change from the 1986 and 1993 versions.

(c) Prohibition of certain disclosure. —

(1) If the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, certifies 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, **no wire or electronic communications service provider**,[19] or officer, employee, or agent thereof, **shall disclose to any person** (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) **that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.**

(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).

(3) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such person of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).

(4) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request under subsection (a).

(d) Dissemination by bureau. —The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement that certain congressional bodies be informed. — On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

(f) Libraries. — A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. § 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic

---

[19] Boldface added by Standler in these three phrases in § 2709(c)(1).

communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) ("electronic communication service") of this title.

18 U.S.C. § 2709 (current September 2007).

Subsections (a) and (d) remain unchanged since the original ECPA in 1986.

Subsection (c), on nondisclosure of NSLs, was modified by the USA PATRIOT Improvement and Reauthorization Act of 2005, Public Law Nr. 109-177 at § 116, 120 Stat. 213-214 (9 March 2006). Note that the recipient of an NSL may now — for the first time since the original ECPA in 1986 — lawfully consult his/her attorney.

Subsection (f), about libraries, was inserted by the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Public Law Nr. 109-178, § 5, 120 Stat. 281 (9 March 2006).

18 U.S.C. § 3511

In March 2006, Congress passed Public Law 109-177, of which § 115 created the following new section in the U.S. Code for judicial review of National Security Letters:

Judicial review of requests for information

(a) The recipient of a request for records, a report, or other information under section 2709(b) of this title,[20] section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act,[21] section 1114(a)(5)(A) of the Right to Financial Privacy Act,[22] or section 802(a) of the National Security Act[23] of 1947 may, in the United States district court for the district in which that person or entity does business or resides, petition for an order modifying or setting aside the request. The court may modify or set aside the request if compliance would be unreasonable, oppressive, or otherwise unlawful.

(b)(1) The recipient of a request for records, a report, or other information under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, may petition any court described in subsection (a) for an order modifying or setting aside a nondisclosure requirement imposed in connection with such a request.

---

[20] Quoted above in this essay.

[21] The Fair Credit Reporting Act is codified at 15 U.S.C.A. § 1681 et seq. (first enacted 1968 and subsequently modified).

[22] The Right to Financial Privacy Act is codified at 12 U.S.C.A. § 3414 (first enacted 1978, subsequently modified).

[23] Codified at 50 U.S.C.A. § 436.

(b)(2) If the petition is filed within one year of the request for records, a report, or other information under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, the court may modify or set aside such a nondisclosure requirement if it 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. If, at the time of the petition, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, or in the case of a request by a department, agency, or instrumentality of the Federal Government other than the Department of Justice, the head or deputy head of such department, agency, or instrumentality, 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.

(b)(3) If the petition is filed one year or more after the request for records, a report, or other information under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, or in the case of a request by a department, agency, or instrumentality of the Federal Government other than the Federal Bureau of Investigation, the head or deputy head of such department, agency, or instrumentality, within ninety days of the filing of the petition, shall either terminate the nondisclosure requirement or re-certify that disclosure may result in a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person. In the event of re-certification, the court may modify or set aside such a nondisclosure requirement if it 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. If the recertification that disclosure may endanger the national security of the United States or interfere with diplomatic relations is made by the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, such certification shall be treated as conclusive unless the court finds that the recertification was made in bad faith. If the court denies a petition for an order modifying or setting aside a nondisclosure requirement under this paragraph, the recipient shall be precluded for a period of one year from filing another petition to modify or set aside such nondisclosure requirement.

(c) In the case of a failure to comply with a request for records, a report, or other information made to any person or entity under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, **the Attorney General may invoke**

the aid of any district court of the United States[24] within the jurisdiction in which the investigation is carried on or the person or entity resides, carries on business, or may be found, **to compel compliance with the request.** The court may issue an order requiring the person or entity to comply with the request. **Any failure to obey the order of the court may be punished by the court as contempt thereof.** Any process under this section may be served in any judicial district in which the person or entity may be found.

(d) In all proceedings under this section, subject to any right to an open hearing in a contempt proceeding, the court must close any hearing to the extent necessary to prevent an unauthorized disclosure of a request for records, a report, or other information made to any person or entity under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947. Petitions, filings, records, orders, and subpoenas must also be kept under seal to the extent and as long as necessary to prevent the unauthorized disclosure of a request for records, a report, or other information made to any person or entity under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947.

(e) In all proceedings under this section, the court shall, upon request of the government, review ex parte and in camera any government submission or portions thereof, which may include classified information.

(current September 2007).

18 U.S.C. § 3511, created by the USA PATRIOT Improvement and Reauthorization Act of 2005, Public Law Nr. 109-177 at § 115, 120 Stat. 211-213 (9 March 2006).

18 U.S.C. § 1510

For many years, there were no criminal penalties for the *un*authorized disclosure of a National Security Letter. In 2006, Congress finally repaired this glaring defect in § 117 of the USA PATRIOT Improvement and Reauthorization Act of 2005, House of Representatives Conference Report 109-333 (8 Dec 2005), which became Public Law Nr. 109-177, 120 Stat. 217 (9 March 2006).

18 U.S.C. § 1510. Obstruction of criminal investigations

....

(e) Whoever, having been notified of the applicable disclosure prohibitions or confidentiality requirements of section 2709(c)(1) of this title, section 626(d)(1) or 627(c)(1) of the Fair Credit Reporting Act (15 U. S.C. § 1681u(d)(1) or § 1681v(c)(1)), section 1114(a)(3)(A) or 1114(a)(5)(D)(i) of the Right to Financial Privacy Act (12 U.S.C. § 3414(a)(3)(A) or § 3414(a)(5)(D)(i)), or section 802(b)(1) of the National Security Act of 1947 (50 U.S.C. § 436(b)(1)), knowingly and with the intent to obstruct an investigation or judicial proceeding

[24] Boldface added by Standler.

violates such prohibitions or requirements applicable by law to such person shall be **imprisoned for not more than five years**,[25] fined under this title, or both.

18 U.S.C. § 1510 (current September 2007).

Court Cases on NSLs

The American Civil Liberties Union provided attorneys for two litigated challenges to National Security Letters. The ACLU website has a large collection of documents on these two cases, one involving records of an Internet Service Provider and the other involving records of a library:

http://www.aclu.org/safefree/nationalsecurityletters/
http://www.aclu.org/safefree/patriot/17458res20040929.html (NSL)
http://www.aclu.org/safefree/nationalsecurityletters/22023res20051130.html (ISP)
http://www.aclu.org/safefree/nationalsecurityletters/25680res20060526.html (library records)

- *Doe v. Ashcroft,* 334 F.Supp.2d 471 (S.D.N.Y. 28 Sep 2004) (injunction issued).

Plaintiff was an anonymous (i.e., "John Doe") Internet Service Provider in New York State who challenged a NSL by suing the U.S. Attorney General in his official capacity. Judge Marrero in the U.S. District Court held that 18 U.S.C. § 2709 violated the 4th Amendment,[26] and that the gag order in § 2709(c) violated the 1st Amendment.

- *Doe v. Gonzales,* 386 F.Supp.2d 66 (D.Conn. 9 Sep 2005) (preliminary injunction issued).

Plaintiff was a library service company in Connecticut who anonymously (i.e., "John Doe")[27] sued the U.S. Attorney General in his official capacity. The trial court issued a preliminary injunction prohibiting the government from enforcing the gag order in NSLs.

- *vacated,* 449 F.3d 415 (2nd Cir. 23 May 2006).

The government appealed both of these cases, and the U.S. Court of Appeals vacated both decisions, because Congress had subsequently amended the statute during the March 2006 renewal of the PATRIOT Act, making the original case moot.

---

[25] Boldface added by Standler.

[26] "Accordingly, the Court concludes that § 2709, as applied here, must be invalidated because in all but the exceptional case it has the effect of authorizing coercive searches effectively immune from any judicial process, in violation of the Fourth Amendment." 334 F.Supp.2d at 506.

[27] *The New York Times* newspaper identified the plaintiff as *Library Connection Inc.* Alison Leigh Cowan, "Four Librarians Finally Break Silence in Records Case," *The New York Times,* http://www.nytimes.com/2006/05/31/nyregion/31library.html (31 May 2006).

- *on remand,* — F.Supp.2d —, 2007 WL 2584559 (S.D.N.Y. 6 Sep 2007)

Judge Marrero again held that the NSL to the Internet Service Provider was *un*constitutional. I will include here some quotations from this opinion when West provides the pagination in the FEDERAL SUPPLEMENT reporter.

Newspaper Articles on NSLs

24 March 2003

Although National Security Letters have been in federal statutes since 1978, the first mention by *The Washington Post* of "National Security Letter" in the context of terrorism investigation occurred in a March 2003 article:

> Since the Sept. 11, 2001, attacks, the Justice Department and FBI have dramatically increased the use of two little-known powers that allow authorities to tap telephones, seize bank and telephone records and obtain other information in counterterrorism investigations with no immediate court oversight, according to officials and newly disclosed documents.
>
> The FBI, for example, has issued scores of "national security letters" that require businesses to turn over electronic records about finances, telephone calls, e-mail and other personal information, according to officials and documents. The letters, a type of administrative subpoena, may be issued independently by FBI field offices and are not subject to judicial review unless a case comes to court, officials said.
>
> Attorney General John D. Ashcroft has also personally signed more than 170 "emergency foreign intelligence warrants," three times the number authorized in the preceding 23 years, according to recent congressional testimony.
>
> ....
>
> The use of national security letters has been accelerated in part because Congress made it easier to use and apply them. The USA Patriot Act, a package of sweeping anti-terrorism legislation passed after the Sept. 11 attacks, loosened the standard for targeting individuals by national security letters and allowed FBI field offices, rather than a senior official at headquarters, to issue them, officials said.
>
> The records that can be obtained through the letters include telephone logs, e-mail logs, certain financial and bank records and credit reports, a Justice official said.
>
> ....
>
> But a November 2001 memorandum prepared by FBI attorneys warned that the letters "must be used judiciously" to avoid angering Congress, which will reconsider Patriot provisions in 2005. "The greater availability of NSLs does not mean they should be used in every case," the memo says.
>
> Beryl A. Howell, former general counsel to Sen. Patrick Leahy (D-Vt.) and a specialist in surveillance law, described national security letters as "an unchecked, secret power that makes it invisible to public scrutiny and difficult even for congressional oversight." Howell now is a managing director and general counsel at Stroz Friedberg LLC, a computer forensic firm in the District.

....

Dan Eggen and Robert O'Harrow Jr., "U.S. Steps Up Secret Surveillance FBI, Justice Dept. Increase Use of Wiretaps, Records Searches," *The Washington Post,* p. A01 (24 March 2003).
http://www.washingtonpost.com/wp-dyn/content/article/2005/11/04/AR2005110401110.html

6 Nov 2005

On 6 November 2005, *The Washington Post* reported on litigation by a library in Connecticut against the FBI's National Security Letters:

> The FBI came calling in Windsor, Conn., this summer with a document marked for delivery by hand. On Matianuk Avenue, across from the tennis courts, two special agents found their man. They gave George Christian the letter, which warned him to tell no one, ever, what it said.
>
> Under the shield and stars of the FBI crest, the letter directed Christian to surrender "all subscriber information, billing information and access logs of any person" who used a specific computer at a library branch some distance away. Christian, who manages digital records for three dozen Connecticut libraries, said in an affidavit that he configures his system for privacy. But the vendors of the software he operates said their databases can reveal the Web sites that visitors browse, the e-mail accounts they open and the books they borrow.
>
> Christian refused to hand over those records, and his employer, Library Connection Inc., filed suit for the right to protest the FBI demand in public. The Washington Post established their identities — still under seal in the U.S. Court of Appeals for the 2nd Circuit — by comparing unsealed portions of the file with public records and information gleaned from people who had no knowledge of the FBI demand.
>
> The Connecticut case affords a rare glimpse of an exponentially growing practice of domestic surveillance under the USA Patriot Act, which marked its fourth anniversary on Oct. 26. "National security letters," created in the 1970s for espionage and terrorism investigations, originated as narrow exceptions in consumer privacy law, enabling the FBI to review in secret the customer records of suspected foreign agents. The Patriot Act, and Bush administration guidelines for its use, transformed those letters by permitting clandestine scrutiny of U.S. residents and visitors who are not alleged to be terrorists or spies.
>
> The FBI now issues more than 30,000 national security letters a year, according to government sources, a hundredfold increase over historic norms. The letters — one of which can be used to sweep up the records of many people — are extending the bureau's reach as never before into the telephone calls, correspondence and financial lives of ordinary Americans.

....

> National security letters offer a case study of the impact of the Patriot Act outside the spotlight of political debate. Drafted in haste after the Sept. 11, 2001, attacks, the law's 132 pages wrought scores of changes in the landscape of intelligence and law enforcement. Many received far more attention than the amendments to a seemingly pedestrian power to review "transactional records." But few if any other provisions touch as many ordinary Americans without their knowledge.
>
> Senior FBI officials acknowledged in interviews that the proliferation of national security letters results primarily from the bureau's new authority to collect intimate facts about people

who are not suspected of any wrongdoing. Criticized for failure to detect the Sept. 11 plot, the bureau now casts a much wider net, using national security letters to generate leads as well as to pursue them. Casual or unwitting contact with a suspect — a single telephone call, for example — may attract the attention of investigators and subject a person to scrutiny about which he never learns.

A national security letter cannot be used to authorize eavesdropping or to read the contents of e-mail. But it does permit investigators to trace revealing paths through the private affairs of a modern digital citizen. The records it yields describe where a person makes and spends money, with whom he lives and lived before, how much he gambles, what he buys online, what he pawns and borrows, where he travels, how he invests, what he searches for and reads on the Web, and who telephones or e-mails him at home and at work.

....

At around the time the FBI found George Christian in Connecticut, agents from the bureau's Charlotte field office paid an urgent call on the chemical engineering department at North Carolina State University in Raleigh. They were looking for information about a former student named Magdy Nashar, then suspected in the July 7 London subway bombing but since cleared of suspicion.

University officials said in interviews late last month that the FBI tried to use a national security letter to demand much more information than the law allows.

David T. Drooz, the university's senior associate counsel, said special authority is required for the surrender of records protected by educational and medical privacy. The FBI's first request, a July 14 grand jury subpoena, did not appear to supply that authority, Drooz said, and the university did not honor it. Referring to notes he took that day, Drooz said Eric Davis, the FBI's top lawyer in Charlotte, "was focused very much on the urgency" and "he even indicated the case was of interest to President Bush."

The next day, July 15, FBI agents arrived with a national security letter. Drooz said it demanded all records of Nashar's admission, housing, emergency contacts, use of health services and extracurricular activities. University lawyers "looked up what law we could on the fly," he said. They discovered that the FBI was demanding files that national security letters have no power to obtain. The statute the FBI cited that day covers only telephone and Internet records.

"We're very eager to comply with the authorities in this regard, but we needed to have what we felt was a legally valid procedure," said Larry A. Neilsen, the university provost.

Soon afterward, the FBI returned with a new subpoena. It was the same as the first one, Drooz said, and the university still had doubts about its legal sufficiency. This time, however, it came from New York and summoned Drooz to appear personally. The tactic was "a bit heavy-handed," Drooz said, "the implication being you're subject to contempt of court." Drooz surrendered the records.

The FBI's Charlotte office referred questions to headquarters. A high-ranking FBI official, who spoke on the condition of anonymity, acknowledged that the field office erred in attempting to use a national security letter. Investigators, he said, "were in a big hurry for obvious reasons" and did not approach the university "in the exact right way."

....

Barton Gellman, "The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans," *The Washington Post,* p. A01 (6 Nov 2005).
http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html

9 March 2007

On 9 March 2007, *The Washington Post* reported:

> A Justice Department investigation has found pervasive errors in the FBI's use of its power to secretly demand telephone, e-mail and financial records in national security cases, officials with access to the report said yesterday.
>
> The inspector general's audit found 22 possible breaches of internal FBI and Justice Department regulations — some of which were potential violations of law — in a sampling of 293 "national security letters." The letters were used by the FBI to obtain the personal records of U.S. residents or visitors between 2003 and 2005. The FBI identified 26 potential violations in other cases.
>
> Officials said they could not be sure of the scope of the violations but suggested they could be more widespread, though not deliberate. In nearly a quarter of the case files Inspector General Glenn A. Fine reviewed, he found previously unreported potential violations.
>
> The use of national security letters has grown exponentially since the Sept. 11, 2001, attacks. In 2005 alone, the audit found, the FBI issued more than 19,000 such letters, amounting to 47,000 separate requests for information.
>
> The letters enable an FBI field office to compel the release of private information without the authority of a grand jury or judge. The USA Patriot Act, enacted after the 2001 attacks, eliminated the requirement that the FBI show "specific and articulable" reasons to believe that the records it demands belong to a foreign intelligence agent or terrorist.
>
> That law, and Bush administration guidelines for its use, transformed national security letters by permitting clandestine scrutiny of U.S. residents and visitors who are not alleged to be terrorists or spies.
>
> Now the bureau needs only to certify that the records are "sought for" or "relevant to" an investigation "to protect against international terrorism or clandestine intelligence activities."
>
> According to three officials with access to the report, Fine said the possible violations he discovered did not "manifest deliberate attempts to circumvent statutory limitations or departmental policies."
>
> But Fine found that FBI agents used national security letters without citing an authorized investigation, claimed "exigent" circumstances that did not exist in demanding information and did not have adequate documentation to justify the issuance of letters.
>
> In at least two cases, the officials said, Fine found that the FBI obtained full credit reports using a national security letter that could lawfully be employed to obtain only summary information. In an unknown number of other cases, third parties such as telephone companies, banks and Internet providers responded to national security letters with detailed personal information about customers that the letters do not permit to be released. The FBI "sequestered" that information, a law enforcement official said last night, but did not destroy it.
>
> ....
>
> Fine's audit, which was limited to 77 case files in four FBI field offices, found that those offices did not even generate accurate counts of the national security letters they issued, omitting about one in five letters from the reports they sent to headquarters in Washington. Those inaccurate numbers, in turn, were used as the basis for required reports to Congress.

> Officials said they believe that the 48 known problems may be the tip of the iceberg in an internal oversight system that one of them described as "shoddy."
>
> The report identified several instances in which the FBI used a tool known as "exigent letters" to obtain information urgently, promising that the requests would be covered later by grand jury subpoenas or national security letters. In several of those cases, the subpoenas were never sent, the review found.
>
> The review also found several instances in which agents claimed there were exigent circumstances when none existed. The FBI recently ended the practice of using exigent letters in national security cases, officials said last night.
>
> ....

John Solomon and Barton Gellman, "Frequent Errors In FBI's Secret Records Requests Audit Finds Possible Rule Violations," *The Washington Post,* p. A01 (9 March 2007)
http://www.washingtonpost.com/wp-dyn/content/article/2007/03/08/AR2007030802356_pf.html

The following day, an Associated Press report was published in *The Washington Post* under the headline "Gonzales, Mueller Admit FBI Broke Law":

> The nation's top two law enforcement officials acknowledged Friday the FBI broke the law to secretly pry out personal information about Americans. They apologized and vowed to prevent further illegal intrusions.
>
> Attorney General Alberto Gonzales left open the possibility of pursuing criminal charges against FBI agents or lawyers who improperly used the USA Patriot Act in pursuit of suspected terrorists and spies.
>
> The FBI's transgressions were spelled out in a damning 126-page audit by Justice Department Inspector General Glenn A. Fine. He found that agents sometimes demanded personal data on people without official authorization, and in other cases improperly obtained telephone records in non-emergency circumstances.
>
> The audit also concluded that the FBI for three years underreported to Congress how often it used national security letters to ask businesses to turn over customer data. The letters are administrative subpoenas that do not require a judge's approval.
>
> ....

Lara Jakes Jordan, Associated Press, "Gonzales, Mueller Admit FBI Broke Law," *The Washington Post,* (06:06 ET 10 Mar 2007)
http://www.washingtonpost.com/wp-dyn/content/article/2007/03/10/AR2007031000324.html

On 11 March 2007, *The Washington Post* published an editorial on this scandal:

> The expansion of law enforcement powers approved by Congress after Sept. 11 and contained in the USA Patriot Act was conditioned on the notion that these new authorities would be carefully used and closely monitored. An infuriating report released Friday by the Justice Department's inspector general, Glenn A. Fine, demonstrates that the Federal Bureau of Investigation treated its new powers with anything but that kind of restraint. The report depicts an FBI cavalierly using its expanded power to issue "national security letters" without adequate oversight or justification.

> National security letters are used to obtain information such as credit and financial data and telephone or e-mail subscriber records (but not the content of messages) without having to secure a court order. The Patriot Act made it far easier for the FBI to use this tool. Now, the information needs to be only "relevant" to a terrorism or espionage case — involving any individual swept up in the case, not just the target — and the heads of FBI field offices can approve the search.
>
> Having obtained these far-reaching new powers, according to the report, the FBI proceeded to "seriously misuse" them. It didn't establish clear guidelines for using national security letters, didn't institute an adequate system for approving requests and didn't put in place procedures to purge information if the investigation fizzled. Although the FBI itself reported to a review board a mere 26 instances in which information was improperly obtained, the real number appears to be much higher. Of just 77 files reviewed by the inspector general, 17 — 22 percent — revealed one or more instances in which information may have been obtained in violation of the law. Indeed, the FBI's procedures were so slipshod, the report concludes, that it didn't even keep proper count of how many such letters were issued. The use of these letters ballooned from 8,500 in 2000 to 47,000 in 2005 — but that "significantly understated" the real numbers, the report found.
>
> Beyond that — and perhaps the most disturbing revelation in a disturbing document — the FBI came up with a category of demands called exigent letters, in which agents got around even the minimal requirements of national security letters. These exigent letters — signed by FBI counterterrorism personnel not authorized to sign national security letters — assured telephone companies on the receiving end that investigators faced an emergency situation and that subpoenas or national security letters would follow. In fact, according to the account of the more than 700 such letters, many times there were no urgent circumstances, and many times the promised follow-up authorization never happened. This lawless practice was so egregious it was stopped last May, FBI Director Robert S. Mueller III announced.

....

Editorial, "Abuse of Authority The FBI's gross misuse of a counterterrorism device," *The Washington Post,* p. B06 (11 March 2007).

A recipient of an NSL discussed the personal effect of the NSL on him:
anonymous, "My National Security Letter Gag Order," *The Washington Post,* p. A17, http://www.washingtonpost.com/wp-dyn/content/article/2007/03/22/AR2007032201882.html (23 March 2007).

9 Sep 2007

While the U.S. Department of Justice was trying to defend 18 U.S.C. § 2709 in court, *The New York Times* published an article indicating that the FBI's use of National Security Letters was much broader than previously publicly reported.

> The F.B.I. cast a much wider net in its terrorism investigations than it has previously acknowledged by relying on telecommunications companies to analyze phone-call patterns of the associates of Americans who had come under suspicion, according to newly obtained bureau records.

The documents indicate that the Federal Bureau of Investigation used secret demands for records to obtain data not only on individuals it saw as targets but also details on their "community of interest" — the network of people that the target was in contact with. The bureau stopped the practice early this year in part because of broader questions raised about its aggressive use of the records demands, which are known as national security letters, officials said.

The community of interest data sought by the F.B.I. is central to a data-mining technique intelligence officials call link analysis. Since the attacks of Sept. 11, 2001, American counterterrorism officials have turned more frequently to the technique, using communications patterns and other data to identify suspects who may not have any other known links to extremists.

The concept has strong government proponents who see it as a vital tool in predicting and preventing attacks, and it is also thought to have helped the National Security Agency identify targets for its domestic eavesdropping program. But privacy advocates, civil rights leaders and even some counterterrorism officials warn that link analysis can be misused to establish tenuous links to people who have no real connection to terrorism but may be drawn into an investigation nonetheless.

Typically, community of interest data might include an analysis of which people the targets called most frequently, how long they generally talked and at what times of day, sudden fluctuations in activity, geographic regions that were called, and other data, law enforcement and industry officials said.

The F.B.I. declined to say exactly what data had been turned over. It was limited to people and phone numbers "once removed" from the actual target of the national security letters, said a government official who spoke on condition of anonymity because of a continuing review by the Justice Department.

The bureau had declined to discuss any aspect of the community of interest requests because it said the issue was part of an investigation by the Justice Department inspector general's office into national security letters. An initial review in March by the inspector general found widespread violations in the F.B.I.'s use of the letters, but did not mention the use of community of interest data.

On Saturday [8 Sep 2007], in response to the posting of the article on the Web site of *The New York Times,* Mike Kortan, a spokesman for the F.B.I., said "it is important to emphasize" that community of interest data is "no longer being used pending the development of an appropriate oversight and approval policy, was used infrequently, and was never used for e-mail communications."

....

The requests for such data showed up a dozen times, using nearly identical language, in records from one six-month period in 2005 obtained by a nonprofit advocacy group, the Electronic Frontier Foundation, through a Freedom of Information Act lawsuit that it brought against the government. The F.B.I. recently turned over 2,500 pages of documents to the group. The boilerplate language suggests the requests may have been used in many of more than 700 emergency or "exigent" national security letters. Earlier this year, the bureau banned the use of the exigent letters because they had never been authorized by law.

The reason for the suspension is unclear, but it appears to have been set off in part by the questions raised by the inspector general's initial review into abuses in the use of national security letters. The official said the F.B.I. itself was examining the use of the community of interest requests to get a better understanding of how and when they were used, but he added that they appeared to have been used in a relatively small percentage of the tens of thousand of

> the records requests each year. "In an exigent circumstance, that's information that may be relevant to an investigation," the official said.
>
> A federal judge in Manhattan last week struck down parts of the USA Patriot Act that had authorized the F.B.I.'s use of the national security letters, saying that some provisions violated the First Amendment and the constitutional separation of powers guarantee. In many cases, the target of a national security letter whose records are being sought is not necessarily the actual subject of a terrorism investigation and may not be suspected at all. Under the Patriot Act, the F.B.I. must assert only that the records gathered through the letter are considered relevant to a terrorism investigation.
>
> Some legal analysts and privacy advocates suggested that the disclosure of the F.B.I.'s collection of community of interest records offered another example of the bureau exceeding the substantial powers already granted it by Congress.
>
> ....

Eric Lichtblau, "F.B.I. Data Mining Reached Beyond Initial Targets," *New York Times,* http://www.nytimes.com/2007/09/09/washington/09fbi.html (9 Sep 2007).

Conclusion

It is appalling that such a blatantly *un*constitutional statute as 18 U.S.C. § 2709 persisted from 1986 until 2004, without challenge in court. It should be an embarrassment to the U.S. Congress that such a statute was passed, and — worse — the *un*constitutional defects were not repaired for more than twenty years.

One lesson of this debacle seems to be that, when Congress makes it easy for government bureaucrats to violate the privacy of U.S. citizens, then the government will enthusiastically violate the privacy of citizens.

Bibliography

Charles Doyle, *Administrative Subpoenas and National Security Letters in Criminal and Foreign Intelligence Investigations: Background and Proposed Adjustments,* Congressional Research Service (15 April 2005), available at: http://www.fas.org/sgp/crs/natsec/RL32880.pdf

Charles Doyle, *National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments*, Congressional Research Service (20 March 2007), available at: http://www.fas.org/sgp/crs/intel/RL33320.pdf (highly recommended)

Electronic Privacy Information Center, National Security Letters (NSLs) website, http://www.epic.org/privacy/nsl/default.html

Sherwood, The Enforcement of Administrative Subpoenas, 44 COLUMBIA LAW REVIEW 531 (1944).

This document is at **www.rbs2.com/NSL.pdf**
My most recent search for court cases on this topic was in September 2007.
created 11 Sep 2007, revised 24 Sep 2007

return to my homepage at http://www.rbs2.com/