



CRS Report for Congress

National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments

Charles Doyle
Senior Specialist
American Law Division

Summary

Five statutory provisions vest government agencies responsible for certain foreign intelligence investigations (principally the Federal Bureau of Investigation [FBI]) with authority to issue written commands comparable to administrative subpoenas. These National Security Letters (NSLs) seek customer and consumer transaction information in national security investigations from communications providers, financial institutions, and credit agencies. Section 505 of the USA PATRIOT Act expanded the circumstances under which an NSL could be used. Subsequent press accounts suggested that their use had become widespread. Two lower federal courts, however, found the uncertainties, practices, and policies associated with the use of NSL authority contrary to the First Amendment right of freedom of speech, and thus brought into question the extent to which NSL authority could be used in the future. The USA PATRIOT Improvement and Reauthorization Act, P.L. 109-177, 120 Stat. 192 (2006) (H.R. 3199), and P.L. 109-178, 120 Stat. 278 (2006) (S. 2271), amend the NSL statutes and related law to address some of the concerns raised by critics and the courts. A report of the Department of Justice's Inspector General found that in its early use of its expanded USA PATRIOT Act authority the FBI had "used NSLs in violation of applicable NSL statutes, Attorney General Guidelines, and internal FBI policies," but that no criminal laws had been broken.

This is an abridged version of CRS Report RL33320, *National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments*, without the footnotes, appendices, and most of the citations to authority found in the longer report.

Background

The ancestor of the first NSL letter provision is an exception to privacy protections afforded by the Right to Financial Privacy Act (RFPA). Its history is not particularly instructive and consists primarily of a determination that the exception in its original form

should not be too broadly construed. But the exception was just that, an exception. It was neither an affirmative grant of authority to request information nor a command to financial institutions to provide information when asked. It removed the restrictions on the release of customer information imposed on financial institutions by the RFPA, but it left them free to decline to comply when asked to do so.

[I]n certain significant instances, financial institutions [had] declined to grant the FBI access to financial records in response to requests under Section 1114(a). The FBI informed the Committee that the problem occurs particularly in States which have State constitutional privacy protection provisions or State banking privacy laws. In those States, financial institutions decline to grant the FBI access because State law prohibits them from granting such access and the RFPA, since it permits but does not mandate such access, does not override State law. In such a situation, the concerned financial institutions which might otherwise desire to grant the FBI access to a customer's record will not do so, because State law does not allow such cooperation, and cooperation might expose them to liability to the customer whose records the FBI sought access. (H.Rept. 99-690, at 15-6 [1986].)

Congress responded with passage of the first NSL statute as an amendment to the RFPA, affirmatively giving the FBI access to financial institution records in certain foreign intelligence cases. At the same time, in the Electronic Communications Privacy Act, it afforded the FBI comparable access to telephone company and other communications service provider customer information. Together, the two NSL provisions afforded the FBI access to communications and financial business records under limited circumstances — customer and customer transaction information held by telephone carriers and banks pertaining to a foreign power or its agents relevant to a foreign counterintelligence investigation. Both the communications provider section and the RFPA section contained nondisclosure provisions and limitations on further dissemination, except pursuant to guidelines promulgated by the Attorney General. Neither had an express enforcement mechanism nor identified penalties for failure to comply with either the NSL or the nondisclosure instruction.

In the mid-1990s, Congress added two more NSL provisions — one permits NSL use in connection with the investigation of government employee leaks of classified information under the National Security Act; the other grants the FBI access to credit agency records pursuant to the Fair Credit Reporting Act, under much the same conditions as apply to the records of financial institutions. The FBI asked for the Fair Credit Reporting Act amendment as a threshold mechanism to enable it to make more effective use of its bank record access authority:

FBI's right of access under the Right of Financial Privacy Act cannot be effectively used, however, until the FBI discovers which financial institutions are being utilized by the subject of a counterintelligence investigation. Consumer reports maintained by credit bureaus are a ready source of such information, but, although such report[s] are readily available to the private sector, they are not available to FBI counterintelligence investigators....

FBI has made a specific showing ... that the effort to identify financial institutions in order to make use of FBI authority under the Right to Financial Privacy Act can not only be time-consuming and resource-intensive, but can also require the use of investigative techniques — such as physical and electronic surveillance, review of

mail covers, and canvassing of all banks in an area — that would appear to be more intrusive than the review of credit reports. (H.Rept. 104-427, at 36 [1996].)

The National Security Act NSL provision authorizes access to credit and financial institution records of federal employees with security clearances who were required to give their consent as a condition for clearance. Passed in the wake of the Ames espionage case, it is limited to investigations of classified information leaks.

Both the Fair Credit Reporting Act section and the National Security Act section contain dissemination restrictions, as well as safe harbor (immunity) and nondisclosure provisions. Neither has an explicit penalty for improper disclosure of the request, but the Fair Credit Reporting Act section expressly authorizes judicial enforcement.

The USA PATRIOT Act amended three of the four existing NSL statutes and added a fifth. In each of the three NSL statutes available exclusively to the FBI — the Electronic Communications Privacy Act section, the Right to Financial Privacy Act section, and the Fair Credit Reporting Act section — section 505 of the USA PATRIOT Act:

- expanded FBI issuing authority beyond FBI headquarter officials to include the heads of the FBI field offices (i.e., Special Agents in Charge [SACs]);
- eliminated the requirement that the record information sought pertain to a foreign power or the agent of a foreign power;
- required instead that the NSL request be relevant to an investigation to protect against international terrorism or foreign spying; and
- added the caveat that no such investigation of an American can be predicated exclusively on First Amendment-protected activities.

The amendments allowed NSL authority to be employed more quickly (without the delays associated with prior approval from FBI headquarters) and more widely (without requiring that the information pertain to a foreign power or its agents).

Subsection 358(g) of the USA PATRIOT Act amended the Fair Credit Reporting Act to add a fifth and final NSL section, and the provision had one particularly noteworthy feature: it was available not merely to the FBI but to any government agency investigating or analyzing international terrorism:

Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish a consumer report of a consumer and all other information in a consumer's file to a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism when presented with a written certification by such government agency that such information is necessary for the agency's conduct or such investigation, activity or analysis.

Although the subsection's legislative history treats it as a matter of first impression, Congress's obvious intent was to provide other agencies with the national security letter authority comparable to that enjoyed by the FBI under the Fair Credit Reporting Act. The new section had a nondisclosure and a safe harbor subsection, but no express means of judicial enforcement or penalties for improper disclosure of a request under the section.

NSLs in Court

NSLs have rarely been the subject of litigation, but in *Doe v. Ashcroft* and *Doe v. Gonzales*, two lower federal courts suggested that the NSL statutes could not withstand constitutional scrutiny unless more explicit provisions were made for judicial review and permissible disclosure by recipients. In essence, *Doe v. Ashcroft* found that the language of the communications NSL and the practices surrounding its use offended (1) the Fourth Amendment because in all but the exceptional case it has the effect of authorizing coercive searches effectively immune from any judicial process, and (2) the First Amendment because its sweeping, permanent gag order provision applies in every case, to every person, in perpetuity, with no vehicle for the ban to ever be lifted from the recipient or other persons affected under any circumstances, either by the FBI itself, or pursuant to judicial process. Although it did not address the Fourth Amendment issue, *Doe v. Gonzales* reached much the same conclusion on the First Amendment issue: narrowly defined, the government's interest was not compelling; broadly defined, the restraints and restrictions of section 2709(c) that served that interest lacked the narrow tailoring necessary to survive constitutional strict scrutiny. The *Doe* cases addressed only communications NSLs, but the characteristics that tripped the court's suspicions were common to all.

NSL Amendments in the 109th Congress

Both USA PATRIOT Act reauthorization statutes — P.L. 109-177(H.R. 3199) and P.L. 109-178 (S. 2271) — amend the NSL statutes. They provide for judicial enforcement of the letter requests and for judicial review of both the requests and accompanying nondisclosure requirements. They establish specific penalties for failure to comply or to observe the nondisclosure requirements. They make it clear that the nondisclosure requirements do not preclude a recipient from consulting an attorney. They provide a mechanism to lift the nondisclosure requirement. Finally, they expand congressional oversight and call for an Inspector General's audit of use of the authority.

Comparison of NSL Attributes

The following table summarizes the differences among the five NSL sections:

- Section 1114(a)(5) of Right to Financial Privacy Act (12 U.S.C. 3414);
- Sections 626 and 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u, 1691v);
- Section 2709 of the title 18 of the United States Code (18 U.S.C. 2709);
and
- Section 802 of the National Security Act (50 U.S.C. 436).

NSL Statute	18 U.S.C. 2709	12 U.S.C. 3414	15 U.S.C. 1681u	15 U.S.C. 1681v	50 U.S.C. 436
Addressee	communications providers	financial institutions	consumer credit agencies	consumer credit agencies	financial institutions, consumer credit agencies, travel agencies
Certifying officials	senior FBI officials and SACs	senior FBI officials and SACs	senior FBI officials and SACs	supervisory official of an agency investigating, conducting intelligence activities relating to or analyzing int'l terrorism	senior officials no lower than Ass't Secretary or Ass't Director of agency w/ employees w/ access to classified material
Information covered	identified customer's name, address, length of service, and billing info	identified customer financial records	identified consumer's name, address, former address, place and former place of employment	all information relating to an identified consumer	all financial information relating to consenting, identified employee
Standard/purpose	relevant to an investigation to protect against int'l terrorism or clandestine intelligence activities	sought for foreign counter-intelligence purposes to protect against int'l terrorism or clandestine intelligence activities	sought for an investigation to protect against int'l terrorism or clandestine intelligence activities	necessary for the agency's investigation, activities, or analysis of int'l terrorism	necessary to conduct a law enforcement investigation, counter-intelligence inquiry or security determination
Dissemination	only per Att'y Gen. guidelines	only per Att'y Gen. guidelines	w/i FBI, to secure approval for intell. investigation, to military investigators when inform. relates to military member	no statutory provision	only to agency of employee under investigation, DOJ for law enforcement or intell. purposes, or fed. agency when clearly relevant to mission
Immunity/fees	no provisions	no provisions	fees; immunity for good faith compliance with a NSL	immunity for good faith compliance with a NSL	reimbursement; immunity for good faith compliance with a NSL

Inspector General's Report

Section 119 of the USA PATRIOT Improvement and Reauthorization Act, P.L. 109-177, 120 Stat. 219 (2006), instructed the Department of Justice's Inspector General to review and report on the FBI's use of NSLs. In early March 2007, the Inspector General released the first of two required reports that covered calendar years 2003 through 2005, U.S. Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters*, available on March 12, 2007 at [<http://www.usdoj.gov/oig/special/s0703b/final.pdf>]. The second report, covering the time period through the end of calendar year 2006, is due before the end of 2007, P.L. 109-177, §119(c)(2), 120 Stat. 220 (2006).

The Report notes that FBI use of NSLs has increased dramatically, expanding from 8500 requests in 2000 to 47,000 in 2005. Seventy-four percent were issued in conjunction with counter-terrorism investigations, most of the rest in connection with counterintelligence investigations and less than 1 percent as part of foreign computer intrusion investigations. During the three years under review, the percentage of NSLs used to investigate Americans ("U.S. persons") increased from 39% in 2003 to 53% in 2005. A substantial majority of the requests involve records relating to telephone or e-mail communications.

While the Report found no criminal violations, it is somewhat 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. In addition, we found that the FBI circumvented the requirements of the ECPA NSL statute when it issued at least 739 "exigent letters" to obtain telephone toll billing records and subscriber information from three telephone companies without first issuing NSLs. Moreover, in a few other instances, the FBI sought or obtained telephone toll billing records in the absence of a national security investigation, when it sought and obtained consumer full credit reports in a counterintelligence investigation, and when it sought and obtained financial records and telephone toll billing records without first issuing NSLs. *Id.* at 124.