WebMemo
Published by The Heritage Foundation
No. 1853
March 14, 2008

# National Security Letters: Three Important Facts

*Charles D. Stimson and Andrew M. Grossman*

National security letters (NSLs) "continue to be important tools in the FBI's national security investigations," according to a major audit of NSL use released yesterday.[1] The audit, commissioned by Congress and undertaken by the Office of the Inspector General (OIG) of the Department of Justice, is meant to uncover any abuses, errors, or shortcomings in the use of NSLs.[2] This year's audit report, issued one year after the first such report, commends the FBI for making "significant progress" in implementing recommendations from the previous report and the FBI leadership for making it a "top priority" to correct mistakes in the use of NSLs.[3]

Despite the high praise for ongoing compliance efforts and strong numbers (84 possible violations out of about 50,000 requests) in this year's report, critics will predictably assert that privacy violations from NSLs are widespread and significant. But the two reports, taken together, show otherwise. Though both reports show that the FBI has sometimes struggled to measure up to its own standards in using NSLs, they also reveal that incidents of misuse were infrequent and unintentional and did not involve any criminal misconduct. In many cases, misuse was actually due to third parties supplying information beyond the scope of the NSL request, not to any action by the FBI.

Like last year's report, this year's report criticizes the Bureau for failing to follow applicable statutes, guidelines, and internal policies in some cases. The OIG notes, however, that because only one year has passed since the issuance of its first NSL report, it is too early for the FBI's corrective measures made since then to be reflected in the data.[4]

While the FBI won praise for its efforts to improve its use of NSLs, the audit notes that Congress has failed to act on a small but significant recommendation from last year's report that would clarify the scope and applicability of NSLs in the telecommunications domain.[5] The Department of Justice submitted draft legislative language in just four months, but Congress has not taken up the matter in the seven months since then.[6]

NSLs serve very narrow but important counterterrorism and counterintelligence purposes. As explained below, because of the kinds of information that can be sought with NSLs, they are not searches that trigger Fourth Amendment protections and so do not require a warrant. NSLs are very limited in the amount of information they can request, serve as a highly effective substitute for more invasive intelligence operations, and have a long and largely uncontroversial history. They were used long before 9/11 and have been subject to extensive congressional oversight.

This paper, in its entirety, can be found at:
*www.heritage.org/Research/LegalIssues/wm1853.cfm*

Produced by the Center for Legal and Judicial Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

Understanding the following three facts about NSLs is key to any informed discussion of their use and propriety.

Fact No. 1: NSLs predate 9/11, have a long history, and have been subject to extensive congressional oversight.

NSLs date back to the 1978 Right to Financial Privacy Act (RFPA). The first NSL provision excepted "foreign counter- or foreign positive-intelligence activities" from privacy protections restricting financial institutions from disclosing customer information.[7] Financial institutions, however, were not required to cooperate with requests in foreign-intelligence investigations.

In response to complaints from the FBI that state privacy laws were hindering its ability to use the 1978 exception, Congress amended the RFPA to create an affirmative authority to access business records for national security purposes in its 1986 intelligence authorization legislation. The provision mandated that financial institutions provide records at the request of the FBI Director, who must certify that the records are sought for counterintelligence purposes and relate to a believed "foreign power" or "agent of a foreign power."[8]

In addition, the RFPA amendment expressly prohibited disclosure of such requests by financial institutions or their agents. It also required that dissemination of information obtained via NSLs be limited by Attorney General guidelines and required the Attorney General to report to Congress's Intelligence Committees on the use of these NSLs every six months—a requirement included in subsequent NSL statutes.

Since 1986, the basic law governing NSLs has changed only slightly. Since the creation of the RFPA NSL, Congress has created four additional NSLs within three statutes:

- The Electronic Communications Privacy Act (ECPA): This NSL allows the FBI to request the subscriber information (e.g., name, address, telephone number), but not toll records (e.g., who was called), of individuals who are believed to have used a telecommunications provider's services to communicate with a suspected terrorist or person engaged in illegal clandestine intelligence or with a foreign power or agent of a foreign power concerning international terrorism or clandestine intelligence.[9]
- The National Security Act: When requested by the FBI, this NSL requires financial institutions, consumer reporting agencies, and travel agencies to provide records on current and former government employees suspected of leaking classified information to foreign powers and who have consented to permit access to their financial records. It was created in the wake of the Aldrich Ames espionage case to "serve as a deterrent to espionage for financial again" and to aid in espionage investigations.[10]
- The Fair Credit Reporting Act (FCRA): This NSL requires credit bureaus to respond to requests made by the FBI Director for the identities of financial institutions at which a suspected foreign power or agent of a foreign power has maintained an account any for any such individual's identifying information (name, address, etc.).[11]

1. OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (March 2008), *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf [hereinafter 2008 REPORT].
2. Pub. L. 109-177, § 119.
3. 2008 REPORT, *supra* note 1, at 6, 15.
4. *Id.* at 8.
5. *Id.*
6. *Id.* at 32–33.
7. 12 U.S.C. § 3414(a)(1)(A).
8. Pub. L. 99-569, § 404. The relevant provision was codified at 12 U.S.C. § 3414 (a)(5)(A) (1988 ed.).
9. Pub. L. 103-142, § 1 (1993); 18 U.S.C. § 2709 (1994 ed.).
10. H.Rept. 103-541, at 53-54 (1994).


The Heritage Foundation LEADERSHIP FOR AMERICA

- The Fair Credit Reporting Act: This NSL provides all federal agencies that investigate terrorism or conduct terrorism-related intelligence activities with NSL authority similar to that granted to the FBI by the other FCRA NSL. This is the only NSL that was created by the Patriot Act.

Congress has enacted legislation concerning NSLs about one dozen times and has debated changes in them many more times. The first significant, though not major, revisions in NSL authorities were a part of the Patriot Act, which:

1. Granted the leaders of FBI field offices the authority to issue NSLs;
2. Replaced the requirement that information sought must pertain to a foreign power or agent of a foreign power with the requirement that information sought must pertain to investigations "to protect against international terrorism or clandestine intelligence activities," a potentially narrower scope of application; and
3. Mandated that NSLs not be issued in investigations of U.S. persons "conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States."

In sum, the Patriot Act's changes in NSLs were rather narrow and intended to correct an inconsistency between terrorism investigations at different stages of development that would probably have prevented their use in investigations of the 9/11 hijackers. Prior to the Patriot Act, NSLs could not be used to investigate domestic terrorist cells without a known link to a foreign power, even though the types of records obtained via NSLs would be among those most likely to establish a link to a foreign power. The Patriot Act closed this intelligence gap.

In the years since the Patriot Act's passage, Congress has received extensive reporting on their use, as required by statute; has been briefed on the topic multiple times by FBI and other officials; and has requested and received detailed information on their use. This oversight activity led to two additional legislative acts, both passed in 2006, that added additional protections to the NSL process. Those laws are discussed below.

Fact No. 2: NSLs help the FBI to "connect the dots" by using the least invasive and most effective means possible.

As noted in each of the two OIG reports, NSLs have proven to be invaluable tools in counterterrorism and counterintelligence investigations. According to the FBI, the principal uses of NSLs are to:

- Establish evidence to support FISA applications for electronic surveillance, physical searches, or pen register/trap and trace orders;
- Assess communication or financial links between investigative subjects or others;
- Collect information sufficient to fully develop national security investigations;
- Generate leads for other field divisions, Joint Terrorism Task Forces, and other federal agencies or to pass to foreign governments;
- Develop analytical products for distribution within the FBI;
- Develop information that is provided to law enforcement authorities for use in criminal proceedings;
- Collect information sufficient to eliminate concerns about investigative subjects and thereby close national security investigations; and
- Corroborate information derived from other investigative techniques. [12]

Information obtained from each type of NSL has allowed investigators to crack cases, especially in the realms of counterterrorism and counterintelligence. A brief examination of the success stories outlined in the OIG reports under each type of NSL proves the point. The following examples, excerpted from the OIG report, show how counterterrorism and counterintelligence investigations are supported through the lawful use of NSLs:

- Telephone Toll Billing Records. A subject owned a company in the United States and traveled to a foreign country at the behest of a foreign

11. Pub. L. 104-93, § 601 (1996); 15 U.S.C. § 1681u.

12. 2008 REPORT, *supra* note 1, at 6.

intelligence service. In addition, the subject had been collecting telephone records and passing the records to a foreign intelligence officer located in the United States. Through toll billing records obtained from NSLs, the FBI was able to demonstrate that the foreign country's U.S.-based intelligence officer was in contact with the subject. The counterintelligence investigation led to the conviction of a representative of a foreign power.[13]

- Financial Records. Terrorists require money from various sources to finance their operations. Tracking the money has proven to be difficult because terrorists are quite sophisticated in their financial dealings. The FBI needs a sophisticated tool to track suspected terrorist financial activity. The NSLs authorized under the Right to Financial Privacy Act allow the FBI to track down the enemy through their financial transactions.

  The FBI conducted a multi-jurisdiction counterterrorism investigation of convenience store owners in the United States who allegedly sent funds to known Hawaladars in the Middle East. The funds were transferred to suspected al-Qaeda affiliates. The possible violations committed by the subjects of these cases included money laundering, sale of untaxed cigarettes, check cashing fraud, and other fraud-related offenses. The FBI issued national security letters for the store owners' back account records. The records showed that two persons received millions of dollars from the subjects and that another subject had forwarded large sums of money to one of these individuals. The back analysis identified sources and receipts of the money transfers and assisted in the collection of information on targets of the investigation overseas.[14]

- Consumer Credit Reports. During a counterintelligence investigation, the FBI issued an FCRA NSL seeking financial institution and consumer identifying information about an investigative subject who the FBI was told had been recruited to provide sensitive information to a foreign power. The information obtained from the NSL assisted the FBI in eliminating concerns that the subject was hiding assets or laundering funds or that he had received covert payments from the foreign power.[15]

- Toll and Financial Records.

  1. A field office opened a counterterrorism investigation in the spring of 2006 and issued numerous ECPA and RFPA NSLs to communications providers and financial institutions. These NSLs assisted the investigators in confirming the identities of the subjects and were used in support of an application for authority to use additional investigative techniques. NSLs also identified financial institutions that the subjects used, which in turn led to the discovery of certain purchases.[16]
  2. In 2006, while investigating a plot to conduct terrorist activities, a field office served ECPA and RFPA NSLs to obtain financial, telephone subscriber, and telephone toll records for the subjects and their associates. Using this information, investigators identified the financial associates of several of the investigator's subjects while ruling out the possibility that a larger terrorist organization was financing the plot.[17]

As these examples illustrate, NSLs are an extremely effective method of obtaining basic data that are crucial to discovering, monitoring, and undermining terrorist activities. They can also be used to exonerate and are frequently used in place of more invasive methods, such as surveillance, searches, and seizures, that are authorized by law and often applicable.

13. OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS 49 (March 2007).
14. *Id.* at 50.
15. *Id.* at 51.
16. 2008 REPORT, *supra* note 1, at 115.
17. *Id.*

Fact No. 3: NSLs are narrowly tailored and subject to more and stronger procedural protections and oversight than ever before.

The kind of information that the government may obtain from the use of NSLs is far more limited than many realize. Contrary to popular misconceptions, the government cannot use NSLs to wiretap, to access e-mails, or to conduct any kind of surveillance. Rather, NSLs allow the government to retrieve the sort of mundane business records that, while exposing little or no personal information, are extremely useful in uncovering terrorist activities. These records include lists of financial accounts, some bank records, and telephone subscriber information and toll records.

Though some citizens believe that these types of records should be obtained only with a court-issued warrant, the Supreme Court has stated clearly that the Fourth Amendment is not implicated when these types of ordinary business records are shared with the government.[18] The Court has reasoned that when citizens open business accounts and create business records, they hold no reasonable expectation of privacy in the existence of the accounts and records. In many cases, this is intuitive: For example, a major piece of evidence in the trial of Scott Peterson for the murder of his wife was a receipt from the hardware store he visited shortly before the murder to purchase a bag of cement, which prosecutors alleged he used to make anchors to sink his wife's body.[19]

This sort of evidence is routinely obtained with little oversight in police and grand jury investigations. Unlike with NSLs, however, obtaining documents in such investigations requires no signoffs from high-level officials who could be held accountable for misuse and no reporting or auditing. Convening grand juries is time-consuming, expensive, and otherwise cumbersome, however, making them unsuitable for national security investigations. They also offer far fewer procedural protections than NSLs.

Further, despite the limited scope of information that is retrievable with NSLs, they are actually subject to greater privacy protections, by statute, regulation and practice, than ever before.

The USA Patriot Improvement and Reauthorization Act, passed in 2006, added a means to enforce and contest all NSL requests and the nondisclosure requirements accompanying them.[20] 18 U.S.C. § 3511 gave NSL addressees the right to petition a district court to modify or set aside the NSL or its nondisclosure requirement if compliance would be "unreasonable, oppressive, or otherwise unlawful."[21]

The law also amended all five NSLs to clarify the use and scope of nondisclosure requirements.[22] This provision made nondisclosure requirements applicable on a case-by-case basis (previously, all NSLs had been automatically subject to the nondisclosure requirement) upon certification by a high-ranking FBI, Justice Department, or issuing agency officer that disclosure would endanger an investigation or diplomatic relations or endanger a person's life or safety. In that case, the NSL must notify the addressee of the requirement, and the addressee may disclose the NSL for purposes of compliance or to an attorney to contest the NSL.

Third, the law clarified and beefed up reporting requirements, which had differed for each of the NSLs.[23] In addition, it commissioned audits of the use of NSLs.[24]

The second law passed in 2006, the USA Patriot Act Additional Reauthorizing Amendments Act,

18. U.S. v. Miller, 425 U.S. 435, 440–443 (1976).
19. Associated Press, *Peterson Lawyers Prep Closing Arguments*, Oct. 28, 2004, at http://www.foxnews.com/story/0,2933,136898,00.html.
20. Pub. L. 109-177 (2006), § 115; 18 U.S.C. § 3511.
21. 18 U.S.C. §§ 3511 (a), (b)(1).
22. P.L. 109-177 (2006), § 116.
23. P.L. 109-177 (2006), § 118.
24. P.L. 109-177 (2006), § 119.

amended the ECPA to exclude libraries from the definition of "electronic communications provider," making the ECPA NSL entirely inapplicable to libraries.[25]

Statutory law is only the beginning of the protections built in to the NSL process. As the OIG report details, "The FBI has issued needed guidance on the proper use of NSLs" that includes "numerous NSL policies and guidance memoranda that include the proper usage of NSLs and statutory and procedural authorizations and restrictions…; the requirement for sufficient and independent supervisory and legal reviews; and the procedures for identifying and reporting possible intelligence violations."[26]

Further, the FBI has established an institutional body to monitor and improve compliance. The new Office of Integrity and Compliance has the mandate "to ensure that national security investigations and other FBI activities are conducted in a manner consistent with appropriate laws, regulations, and policies," such as those described above.[27] Though it suggests that the Office should have a larger staff, the OIG report considers the establishment of the Office to be a major positive step that will provide "a process for identifying compliance requirements and risks, assessing existing control mechanisms, and developing and implementing better controls to ensure proper use of NSLs."[28]

Finally, a Department of Justice working group reviews "how NSL-derived information is used and retained…with special emphasis on the protection of privacy interests."

In sum, there are extensive judicial, statutory, regulatory, and institutional protections in place to ensure that NSLs are not misused and do not violate Americans' privacy rights. With the number of NSLs issued every year, it is inevitable that there will be some mistakes; but as the OIG report recognizes, the FBI has taken major steps to improve protections and reduce their number.

Conclusion. Congress authorized the FBI to use NSLs in counterterrorism and counterintelligence investigations. Both OIG reports related to the FBI's use of NSLs unequivocally state that NSLs are an indispensable tool in national security investigations. Law enforcement officials, working closely with the intelligence community, need the tools contained within those authorized NSLs to keep Americans safe and to prevent future terrorist attacks.

As the latest OIG report highlights, FBI Director Robert Mueller has made it a top priority to reduce the accidental misuse of NSLs, and the Department of Justice has made significant progress in doing so since the issuance of the 2007 OIG report. Although the report notes the significant progress the Department has made in the past 12 months, it is too early to tell how effective the new systems and controls will be in achieving the ultimate goal of eliminating all inadvertent misuses of NSLs.

*—Charles D. Stimson is Senior Legal Fellow, and Andrew M. Grossman is Senior Legal Policy Analyst, in the Center for Legal and Judicial Studies at The Heritage Foundation.*

25. 18 U.S.C. § 2709 (f).
26. 2008 REPORT, *supra* note 1, at 7.
27. *Id.*
28. *Id.*