National Security Letters: Proposed Amendments in the 111th Congress

Charles Doyle
Senior Specialist in American Public Law

October 28, 2009

Congressional Research Service
7-5700
www.crs.gov
R40887

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Five federal statutes authorize various intelligence agencies to demand, through National Security Letters (NSLs), certain customer information from communications providers, financial institutions, and consumer credit reporting agencies, under the Right to Financial Privacy Act, the Fair Credit Reporting Act, the National Security Act, and Electronic Communications Privacy Act. The USA PATRIOT Act expanded NSL authority. Later reports of the Department of Justice Inspector General indicated that (1) the FBI considered the expanded authority very useful; (2) after expansion the number of NSLs requests increased dramatically; (3) the number of requests relating to Americans increased substantially; and (4) FBI use of NSL authority had sometimes failed to comply with statutory, Attorney General, or FBI policies.

Originally, the NSL statutes authorized nondisclosure requirements prohibiting recipients from disclosing receipt or the content of the NSL to anyone, ever. They now permit judicial review of these secrecy provisions. As understood by the courts, recipients may request the issuing agency to seek and justify to the court the continued binding effect of any secrecy requirement.

Several USA PATRIOT Act provisions are scheduled to expire on December 31, 2009. The NSL statutory provisions are not among them. Nevertheless, several bills have been introduced which would amend and in some cases repeal NSL authority. The bills include (1) the National Security Letter Reform Act of 2009 (H.R. 1800), introduced by Representative Nadler; (2) the USA PATRIOT Amendments Act of 2009 (H.R. 3845), introduced by Representative Conyers; (3) the Judicious Use of Surveillance Tools in Counterterrorism Efforts Act of 2009 (JUSTICE Act) (S. 1686), introduced by Senator Feingold; and (4) the USA PATRIOT Act Sunset Extension Act of 2009 (S. 1692), introduced by Senator Leahy and reported to the floor by the Senate Judiciary Committee, S.Rept. 111-92.

In addition to sunset and repeal, the bills raise issues involving amendment of nondisclosure requirements; the promulgation of standards to minimize capturing, using, and holding (long term) NSL generated information, continued periodic IG audits and reports, and limitations on statutory provisions thought by some to permit circumvention of NSL statutory requirements.

This report includes a chart comparing the provisions of the bills and current law. It also reprints the text of the five NSL statutes as they now appear and as they appeared prior to amendment by the USA PATRIOT Act (to which form they would return under some of the bills).

Contents

Tables

Contacts

Introduction

National security letters (NSL) are roughly comparable to administrative subpoenas. Intelligence agencies issue them for intelligence gathering purposes to telephone companies, Internet service providers, consumer credit reporting agencies, banks, and other financial institutions, directing the recipients to turn over certain customer records and similar information. Four bills, introduced in the 111th Congress, propose substantial changes in the law governing NSL authority: H.R. 1800, the National Security Letters Reform Act of 2009 (Rep. Nadler); H.R. 3845, the USA PATRIOT Amendments Act of 2009 (Rep. Conyers); S. 1686, the Judicious Use of Surveillance Tools in Counterterrorism Efforts Act (JUSTICE Act) of 2009 (Sen. Feingold); and S. 1692, the USA PATRIOT Act Sunset Extension Act of 2009 (Sen. Leahy). The Senate Judiciary Committee sent an amended version of S. 1692 to floor on October 13, 2009, 155 *Cong. Rec.*S10361 (daily ed. Oct. 13, 2009), with a report on October 28, 2009, 155 *Cong. Rec.*S10850 (daily ed. Oct. 28, 2009).[1]

The Feingold bill would repeal immediately one of the existing NSL statutes, section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v), created in the USA PATRIOT Act.[2] The Leahy bill would repeal section 627 effective December 31, 2013 and on that date would return the other NSL statutes to their pre-USA PATRIOT Act form.[3] The Conyers bill would return all five NSL statutes to pre-USA PATRIOT Act form effective December 31, 2013, thereby effectively repealing section 627.[4] The Nadler bill would return all but the National Security Act statute (50 U.S.C. 436) to their pre-USA PATRIOT Act form after five years;[5] which has the effect of repealing section 627, the NSL created by the USA PATRIOT Act. While the Nadler bill deals exclusive with NSL matters, the Leahy bill addresses other national security issues, as do the Feingold and Conyers bills, which also speak to related law enforcement issues.[6]

Background

Prior to the USA PATRIOT Act, the NSL statutes were four. One, 18 U.S.C. 2709, obligated communications providers to supply certain customer information upon the written request of the Director of the Federal Bureau of Investigation (FBI) or a senior FBI headquarters official.[7] When customer identity, length of service, and toll records were sought, the letters had to certify (1) that the information was relevant to a foreign counterintelligence investigation and (2) that specific and articulable facts gave reason to believe the information pertained to a foreign power or its agents.[8] When only customer identity and length of service records (but not toll records) were

[1] For purposes of this report, S. 1692 and the Leahy bill refer to the bill as reported out unless otherwise noted; citations to H.R. 1800, the Nadler bill; H.R. 3845, the Conyers bill; or S. 1686, the Feingold bill, refer to those bills as introduced.

[2] S. 1686, §101(c)(2).

[3] S. 1692, §2(c).

[4] H.R. 3845, §202.

[5] H.R. 1800, §5.

[6] This report is limited to a discussion of the NSL proposals in the three bills as introduced.

[7] 18 U.S.C. 2709(a), (b) (2000 ed.).

[8] 18 U.S.C. 2709(b)(1) (2000 ed.).

sought, the letters had to certify (1) again that the information was relevant to a foreign counterintelligence investigation, but (2) that specific and articulable facts gave reason to believe that the customer information pertained to use of the provider's facilities to communicate with foreign powers, their agents or those engaged in international terrorism or criminal clandestine intelligence activities.[9]

In like manner a second statute, section 1114(a)(5) of the Right to Financial Privacy Act, obligated financial institutions to provide the FBI with customers' financial records upon written certification of the FBI Director or his designee (1) that the records were sought for foreign counterintelligence purposes and (2) that specific and articulable facts gave reason to believe that the records were those of a foreign power or its agents.[10]

And so it was with a third, section 626 of the Fair Credit Report Act, which obligated consumer credit reporting agencies to provide customer identification, and the names and addresses of financial institutions at which a designated consumer maintained accounts.[11] Here too, the obligation was triggered by written certification of the FBI Director or his designee (1) that the information was necessary for a foreign counterintelligence investigation, and (2) that specific and articulable facts gave reason to believe that the consumer was either a foreign power, a foreign official, or the agent of a foreign power and was engaged in international terrorism or criminal clandestine intelligence activities.[12]

The fourth, section 802 of the National Security Act, was a bit different.[13] It reached a wider range of potential recipients at the demand of large group of federal officials, but for a more limited purpose. It rested the obligation to provide consumer reports, together with financial information and records, upon consumer reporting agencies, financial agencies, and financial institutions, or holding companies.[14] The requirement was triggered by the certification of senior officials of law enforcement and intelligence agencies, but confined to information pertaining to federal employees with access to classified information and being sought for clearance purposes and inquiries into past or potential security leaks.[15]

USA PATRIOT Act

Section 505 of the USA PATRIOT Act altered the FBI's NSL authority under section 2709, the Right to Financial Privacy Act, and the Fair Credit Reporting Act in several ways:

- It expanded issuing authority to include the heads of FBI field offices (special agents in charge (SACs));
- It eliminated the requirement of specific and articulable facts demonstrating a nexus to a foreign power or its agents;

[9] 18 U.S.C. 2709(b)(2) (2000 ed.).

[10] 12 U.S.C. 3414(a)(5) (2000 ed,).

[11] 15 U.S.C. 1681u(a), (b) (2000 ed.).

[12] Id.

[13] 50 U.S.C. 436 (2000 ed.).

[14] Id.

[15] Id.

- It required instead that the information was sought for or relevant to various national security investigations; and
- It directed that no NSL related investigation of a "U.S. person" (American citizen or foreign resident alien) be predicated exclusively on First Amendment protected activities.[16]
- The National Security Act NSL section remained unchanged, but section 358(g) of the USA PATRIOT Act added a new Fair Credit Reporting Act NSL section 627, 15 U.S.C. 1681v. The new section obligated consumer reporting agencies to provide consumer information and reports to a federal agency "authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism."[17] Senior federal agency officials were empowered to issue the NSL with a certification that the information was "necessary for the agency's conduct or such investigation, activity, or analysis."[18]

2006 Amendments

Several of the USA PATRIOT Act's intelligence gathering provisions were temporary and originally set to expire after five years.[19] The NSL statutes were not among them, but Congress amended the statutes in the USA PATRIOT Improvement and Reauthorization Act of 2005 and the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 nonetheless.[20] The NSL statute amendments were driven both by sensitivity to an Administration desire for more explicit enforcement authority[21] and by judicial developments which had raised questions as to the statutes' constitutional vitality as then written.[22] The statutes then came with open-ended

---

[16] Thus for example, section 626 of the Fair Credit Report Act, once stated in part that

> The Director or the Director's designee may make such a certification only if [he or she] has determined in writing that – (1) such information is necessary for the conduct of an authorized foreign counterintelligence investigation; and (2) there are specific and articulable facts giving reason to believe that the consumer – (A) is a foreign power . . . or a person who is not United States person . . and is an official of a foreign power; or (b) is an agent of a foreign power and is engaging or has engaged in an act of international terrorism . . . or clandestine intelligence activities that involve or may involve a violation of criminal statutes of the United States, 15 U.S.C. 1681u(a) (2000 ed.).

The USA PATRIOT Act redesignated section 626 as section 625 and the amended provision stated that

> The Director or the Director's designee in a position not lower that Deputy Assistant Director at Bureau headquarters or Special Agent in Charge of a Bureau field office designated by the Director may make such a certification only if [he or she] has determined in writing that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such as investigation of a United Stats person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the Untied States, U.S.C. 1681u(a)(2000 ed. Supp.I).

[17] 15 U.S.C. 1681v(a)(2000 ed. Supp. I).

[18] Id.

[19] Sec. 224, P.L. 107-56, 115 Stat. 295 (2001).

[20] P.L. 109-177, 120 Stat. 192 (2006); P.L. 109-178, 120 Stat. 278 (2006), respectively.

[21] E.g., Anti-Terrorism Intelligence Tools Improvement Act of 2003: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security, 108th Cong., 2d Sess. 7-8 (2004)(prepared statement of U.S. Ass't Att'y Gen. Daniel J. Bryant).

[22] *Doe v. Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004)(First and Fourth Amendment concerns); *Doe v. Gonzales*, 386 F.Supp.2d 66 (D. Conn. 2005)(First Amendment concerns).

nondisclosure provisions which barred recipients from disclosing the fact or content of the NSL – ever or to anyone. Yet, they featured neither a penalty provision should the confidential requirement be breached nor in most cases an enforcement mechanism should a NSL obligation be ignored (the original Fair Credit Report Act statute alone had an explicit judicial enforcement component).

The amendments:

- created a judicial enforcement mechanism and a judicial review procedure for both the requests and accompanying nondisclosure requirements;[23]
- established specific penalties for failure to comply with the nondisclosure requirements;[24]
- made it clear that the nondisclosure requirements did not preclude a recipient from consulting an attorney;[25]
- provided a process to ease the nondisclosure requirement;[26]
- expanded Congressional oversight;[27] and
- called for Inspector General's audits of use of NSL authority.[28]

IG Reports

The First IG Report

The Department of Justice Inspector General audit reports, one released in March of 2007 and the second in March of 2008, were less than totally favorable.[29] The first report noted that FBI use of NSLs had increased dramatically, expanding from 8,500 requests in 2000 to 47,000 in 2005, *IG Report I* at 120. During the 3 years under review, the percentage of NSLs used to investigate Americans ("U.S. persons") increased from 39% in 2003 to 53% in 2005.[30] A substantial majority of the requests involved records relating to telephone or e-mail communications, Id.

[23] 28 U.S.C. 3511.

[24] 28 U.S.C. 3511(c), 18 U.S.C. 1510(e).

[25] 12 U.S.C. 3414((a)(3)(A); 15 U.S.C. 1681v(c)(1), 1681u(d)(1); 18 U.S.C. 2709(c)(1); 50 U.S.C. 436(B)(1).

[26] 28 U.S.C. 3511(b).

[27] P.L. 109-177, §118.

[28] P.L. 109-177, §119.

[29] U.S. Department of Justice, Office of the Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters(IG Report I) (March 2007); A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006 (IG Report II) (March 2008), both available on Sept. 18, 2009 at http://www.usdoj.gov/oig/special/index.htm.

[30] *Id.* A "U.S. person" is generally understood to mean "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(2) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection(a)(1), (2), or (3) of this section," 50 U.S.C. 1801.

The report and the subsequent report a year later provided a glimpse at how the individual NSL statutes were used and why they were considered available. In case of the 18 U.S.C. 2709, the Electronic Communications Privacy Act (ECPA) NSL statute, the reports explained that:

> Through national security letters, an FBI field office obtained telephone toll billing records and subscriber information about an investigative subject in a counterterrorism case. The information obtained identified the various telephone numbers with which the subject had frequent contact. Analysis of the telephone records enabled the FBI to identify a group of individuals residing in the same vicinity as the subject. The FBI initiated investigations on these individuals to determine if there was a terrorist cell operating in the city.[31]

> Headquarters and field personnel told us that the principal objective of the most frequently used type of NSL – ECPA NSLs seeking telephone toll billing records, electronic communication transactional records, or subscriber information (telephone and e-mail) – is to develop evidence to support applications for FISA orders.[32]

The Right to Financial Privacy Act (RFPA) NSL statute, 12 U.S.C. 3414(a)(5), also affords authorities access a wide range of information (bank transaction records v. telephone transaction records) as demonstrated by the instances where it proved useful:

> The FBI conducted a multi-jurisdictional counterterrorism investigation of convenience store owners in the United States who allegedly sent funds to known Hawaladars (persons who use the Hawala money transfer system in lieu of or parallel to traditional banks) 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, illegal sale of pseudoephedrine (the precursor ingredient used to manufacture methamphetamine), unemployment insurance fraud, welfare fraud, immigration fraud, income tax violations, and sale of counterfeit merchandise. [33]

> The FBI issued national security letters for the convenience store owners' bank 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 bank analysis identified sources and recipients of the money transfers and assisted in the collection of information on targets of the investigation overseas.[34]

The Fair Credit Reporting Act NSL statutes, 15 U.S.C. 1681u (FCRAu) and 1681v (FCRAv) can be even more illuminating, "The supervisor of a counterterrorism squad told us that the FCRA NSLs enable the FBI to see 'how their investigative subjects conduct their day-to-day activities, how they get their money, and whether they are engaged in white collar crime that could be relevant to their investigations.'"[35]

Overall, the report notes that the FBI used the information gleaned from NSLs for a variety of purposes, "to determine if further investigation is warranted; to generate leads for other

[31] IG Report I at 49.

[32] *IG Report II* at 65. The Foreign Intelligence Surveillance Act (FISA) authorizes the FBI to apply for court orders in national security cases authorizing electronic surveillance, physical searches, the installation and use of pen registers and trap and trace devices, and access to business records and other tangible property, 50 U.S.C. 1801-1862.

[33] Critics might suggest that these offenses are "possible" in the operation of any convenience store.

[34] IG Report I at 50.

[35] *Id.* at 51.

field offices, Joint Terrorism Task Forces, or other federal agencies; and to corroborate information developed from other investigative techniques."[36] Moreover, information supplied in response to NSLs provides the grist of FBI analytical intelligence reports and various FBI databases.[37]

The report was somewhat critical, however, 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.

More specifically, the Report found that:

- a "significant number of NSL-related possible violations were not being identified or reported" as required;
- the only FBI data collection system produced "inaccurate" results;
- the FBI issued over 700 exigent letters acquiring information in a manner that "circumvented the ECPA NSL statute and violated the Attorney General's Guidelines . . . and internal FBI policy;"
- the FBI's Counterterrorism Division initiated over 300 NSLs in a manner that precluded effective review prior to approval;
- 60% of the individual files examined showed violations of FBI internal control policies;
- the FBI did not retain signed copies of the NSLs it issued;
- the FBI had not provided clear guidance on the application of the Attorney General's least-intrusive-feasible-investigative-technique standard in the case of NSLs;
- the precise interpretation of toll billing information as it appears in the ECPA NSL statute is unclear;
- SAC supervision of the attorneys responsible for review of the legal adequacy of proposed NSLs made some of the attorneys reluctant to question the adequacy of the underlying investigation previously approved by the SAC;
- there was no indication that the FBI's misuse of NSL authority constituted criminal conduct;
- personnel both at FBI headquarters and in the field considered NSL use indispensable; and

[36] *Id.* at 65.

[37] Id.

- information generated by NSLs was fed into a number of FBI systems. *IG Report I* at 121-24.

Exigent Letters

Prior to enactment of the Electronic Communications Privacy Act (ECPA), the Supreme Court held that customers had no Fourth Amendment protected privacy rights in the records the telephone company maintained relating to their telephone use.[38] Where a recognized expectation of privacy exists for Fourth Amendment purposes, the Amendment's usual demands such as those of probable cause, particularity, and a warrant may be eased in the face of exigent circumstances. For example, the Fourth Amendment requirement that officers must knock and announce their purpose before forcibly entering a building to execute a warrant can be eased in the presence of certain exigent circumstances such as the threat of the destruction of evidence or danger to the officers.[39] Satisfying Fourth Amendment requirements, however, does not necessarily satisfy statutory prohibitions.

The ECPA prohibits communications service providers from supplying information concerning customer records unless one of the statutory exceptions applies.[40] There are specific exceptions for disclosure upon receipt of a grand jury subpoena[41] or an NSL.[42] A service provider who knowingly or intentionally violates the prohibition is subject to civil liability,[43] but there are no criminal penalties for the breach.

The Inspector General found that contrary to assertions that "the FBI would obtain telephone records only after it served NSLs or grand jury subpoenas, the FBI obtained telephone bill records and subscriber information prior to serving NSLs or grand jury subpoenas" by using "exigent letters."[44] The FBI responded that it had barred the use of exigent letters, but emphasized that the term "exigent letter" does not include emergency disclosures under the exception now found in 18 U.S.C. 2702(c)(4). Thus, the FBI might request that a service provider invoke that exception to the record disclosure bar "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information," 18 U.S.C. 2702(c)(4).

The Second IG Report

The second IG Report reviewed the FBI's use of national security letter authority during calendar year 2006 and the corrective measures taken following the issuance of the IG's first report. The second Report concluded that:

- "the FBI's use of national security letters in 2006 continued the upward trend . . . identified . . . for the period covering 2003 through 2006;

[38] *Smith v. Maryland*, 442 U.S. 735, 745 (1979)

[39] *Richards v. Wisconsin*, 520 U.S. 385, 391 (1997); *Wilson v. Arkansas*, 514 U.S. 927, 936 (1995).

[40] 18 U.S.C. 2702(c).

[41] 18 U.S.C. 2703(c)(2).

[42] 18 U.S.C. 2709(a).

[43] 18 U.S.C. 2707(a).

[44] IG Report I at 90.

- "the percentage of NSL requests generated from investigations of U.S. persons continued to increase significantly, from approximately 39% of all NSL requests issued in 2003 to approximately 57% of all NSL requests issued in 2006;"
- the FBI and DoJ are committed to correcting the problems identified in *IG Report I* and "have made significant progress in addressing the need to improve compliance in the FBI's use of NSLs;" [and]
- "it [was] too early to definitively state whether the new systems and controls developed by the FBI and the Department will eliminate fully the problems with NSLs that we identified," *IG Report II* at 8-9.

Table 1. Profile of the Current NSL Statutes

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 relating to 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.	no statutory provision	only to agency of employee under investigation, DoJ for law enforcement or intell. purposes, or fed. agency when

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
			relates to military member		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

Secrecy, Judicial Review & the Second Circuit

The current secrecy and judicial review provisions applicable to NSLs must be read in light of the Second Circuit's *John Doe, Inc. v. Mukasey* decision, 549 F.3d 861 (2d Cir. 2008). Under the NSL statutes, secrecy is not absolutely required. Instead NSL recipients are bound to secrecy only upon the certification of the requesting agency that disclosure of the request or response may result in a danger to national security; may interfere with diplomatic relations or with a criminal, counterterrorism, or counterintelligence investigation; or may endanger the physical safety of an individual.[45] A recipient may disclose the request to those necessary to comply with the request and to an attorney the recipient consults for related legal advice or assistance.[46] In doing so, the recipient must advise them of the secrecy requirements.[47] Aside from its attorney the recipient must also identify, at the requesting agency's election, those to whom it has disclosed the request.[48]

Judicial Review of NSLs

Under the statute, 18 U.S.C. 3511, *a recipient may petition the court to modify or extinguish any NSL secrecy requirement* within a year of issuance.[49] Thereafter, it may petition to have the veil of secrecy lifted, although it may resubmit a rejected request only once a year.[50] Section 3511 provides that the court may modify or set aside the restriction if it finds "no reason to believe that disclosure may" endanger national security or personal safety or interfere with diplomatic relations or a criminal, countterrorism, or counterintelligence investigation.[51] The section, however, *binds the court to the assertion of a senior executive branch official that such an adverse consequence is possible*.[52]

In addition to authority to review and set aside NSL nondisclosure requirements, the federal courts also enjoy jurisdiction to review and enforce the underlying NSL requests. Under section 3511, recipients may petition and be granted an order modifying or setting aside an NSL, if the

[45] *E.g.*, 18 U.S.C. 2709(c)(1). The other NSL statutes have comparable provisions.

[46] Id.

[47] *E.g.*, 12 U.S.C. 3414(a)(5)(D)(iii). The other NSL statutes have comparable provisions.

[48] *E.g.*,, 15 U.S.C. 1681u(d)(4). The other NSL statutes have comparable provisions.

[49] 18 U.S.C. 3511(b)(2). As explained below, the Second Circuit opinion requires that the provisions in italics here and at the end of the paragraph be understood in the context of First Amendment demands.

[50] 18 U.S.C. 3511(b)(3).

[51] 18 U.S.C. 3511(b)(2), (3).

[52] Id.

court finds that compliance would be unreasonable, oppressive, or otherwise unlawful.[53] The "unreasonable or oppressive" standard is used for grand jury and other subpoenas issued under the Federal Rules of Criminal Procedure.[54] The Rules afford protection against undue burdens and protect privileged communications.[55] Compliance with a particular NSL might be unduly burdensome in some situations, but the circumstances under which NSLs are used suggest few federally recognized privileges. The Rules also impose a relevancy requirement, but in the context of a grand jury investigation a motion to quash will be denied unless it can be shown that "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant" to the investigation.[56] The authority to modify or set aside a NSL that is "unlawful" affords the court an opportunity to determine whether the NSL in question complies with the statutory provisions under which it was issued. Section 3511 also vests the court with authority to enforce the NSL against a recalcitrant recipient. Failure to comply with the court's order thereafter is punishable as contempt of court.[57] A breach of a confidentiality requirement committed knowingly and with the intent to obstruct an investigation or related judicial proceedings is punishable by imprisonment for not more than five years and/or a fine of not more than $250,000 (not more than $500,000 for an organization).[58]

The Second Circuit has concluded that the procedure can survive First Amendment scrutiny only if it involves the following:

- notice to NSL recipients that they may contest any secrecy order;
- expeditious government petition for judicial review of a secrecy order upon recipient request;
- government burden to establish the validity of its narrowly tailored secrecy order;
- no conclusive weigh may be afforded governmental assertions; and
- recipients may apply or reapply annually for judicial review where the government's burden remains the same.[59]

On remand, the district upheld continuation of the nondisclosure order under the procedure suggested by the Second Circuit.[60]

[53] 18 U.S.C. 3511(a).

[54] F.R.Crim.P. 17(c)(2).

[55] 2 Wright, Federal Practice and Procedure §275 (Crim. 3d ed. 2000).

[56] United States v. R. Enterprises, Inc., 498 U.S. 292, 301 (1991).

[57] 18 U.S.C. 3511(c).

[58] 18 U.S.C. 1510(e), 3571, 3559.

[59] *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 883-84 (2d Cir. 2008).

[60] *Doe v. Holder*, ____ F.Supp. 2d ____ (S.D.N.Y. Aug. 5, 2009); see also *Doe v. Holder*, ____ F.Supp. 2d ____ (S.D.N.Y. Oct. 20, 2009).

Proposed Amendments

Sunset and Repeal

Three provisions governing foreign intelligence investigations sunset on December 31, 2009. The NSL provisions are not among them. Nevertheless, each of the bills propose sunset in one form or another. The Feingold bill would repeal immediately one of the existing NSL statutes, section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v).[61] The Leahy bill would repeal section 627 effective December 31, 2013 and on that date would return the others to their pre-USA PATRIOT Act form.[62] The Conyers bill would return all five NSL statutes to pre-USA PATRIOT Act form effective December 31, 2013, thereby effectively repealing section 627.[63] The Nadler bill would return all but the National Security Act statute (50 U.S.C. 436) to their pre-USA PATRIOT Act form after five years.[64]

The USA PATRIOT Act expanded existing authority under 18 U.S.C. 2709, the Right to Financial Privacy Act, and the Fair Credit Reporting Act.[65] It also created new NSL authority in the form of section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v).[66] It did not expand the reach of the National Security Act NSL statute. A return to the state of the law prior to enactment of the USA PATRIOT Act would have the effect of eliminating the amendments it made in the pre-existing NSL statutes as well as any subsequent amendments, and of repealing section 627.

In general terms for the three pre-existing NSL statutes, the USA PATRIOT Act:

- expanded issuing authority to include the heads of FBI field offices (special agents in charge (SACs));
- eliminated the requirement of specific and articulable facts demonstrating a nexus to a foreign power or its agents;
- required instead that the information was sought for or relevant to various national security investigations; and
- directed that no NSL related investigation of a "U.S. person" (American citizen or foreign resident alien) be predicated exclusively on First Amendment protected activities.[67]

This means that:

- NSLs are more readily available to FBI field agents at a lower level of supervisory control;.

[61] S. 1686, §101(c)(2). The relevant text of the NSL statutes, prior to the effective date of the USA PATRIOT Act and now, is appended.

[62] S. 1692, §2(c).

[63] H.R. 3845, §202.

[64] H.R. 1800, §5.

[65] P.L. 107-56, §505, 115 Stat. 365 (2001).

[66] P.L. 107-56, §358(g), 115 Stat. 327 (2001).

[67] 18 U.S.C. 2709((b), 12 U.S.C. 3414(a)(5)(A), 15 U.S.C. 1681u(a).

- NSLs can be used to obtain information pertaining to individuals two, three, or more steps removed from the foreign power or agent of a foreign power that is the focus of the investigation; and
- NSL-related investigations may not be predicated solely on the basis of activities protected by the First Amendment.

A return to the state of the law prior to the effective date of the USA PATRIOT Act would mean NSLs would have to be approved by the FBI Director or a senior FBI headquarters official, and it would have to be based on specific and articulable facts giving reason to believe that the information sought pertains to a foreign power or agent of a foreign power.[68] A witness at an earlier Congressional hearing indicated that the "specific and articulable" facts standard grew out of the standards employed in counterintelligence investigations and did not always translate well in a counterterrorism context:

> My point is that the "specific and articulable facts" standard was particularly suited to the counterintelligence operations of the era in which it was created. A FBI counterintelligence investigation involved examining a linear connection between a foreign intelligence officer (about whom much was known) and his contacts (potential spies). The information known about the intelligence officer was specific in nature, and could be readily used to meet the NSL legal standards . . . . Unlike the traditional linear counterintelligence case, in which the foreign agent tried to recruit the domestic spy using infrequent and highly secure forms of communication, many counterterrorism cases involved complex networks generating a much larger volume of communication and financial transactions. In counter-terrorism cases, the starting point was often not a clearly identifiable agent of a foreign power (as in counterintelligence); indeed, the relevant "foreign power" was itself an imperfectly understood terrorist organization that might defy precise definition. As a consequence, counter-terrorism investigators often had a far more difficult time meeting the "specific and articulable facts" standard.[69]

The language precluding NSL-related investigations grounded exclusively on the exercise of First Amendment rights would also disappear. It is at best unclear, however, that the First Amendment unaided does not embody a comparable prohibition.

At the first sunset of USA PATRIOT Act provisions, Congress amended each of the NSL statutes in the USA PATRIOT Improvement and Reauthorization Act and the USA PATRIOT Act Additional Reauthorization Amendments Act.[70] The amendments state the grounds upon which the NSLs may be made subject to a secrecy requirement (gag order);[71] advise recipients that the order does not preclude disclosure to the recipient's attorney or to those necessary for execution of the request; and notify recipients of their right to judicial review of the order.[72] They too would disappear were the law carried back to its pre-USA PATRIOT Act state.

---

[68] 18 U.S.C. 2709((b)(2000 ed.), 12 U.S.C. 3414(a)(5)(A)(2000 ed.), 15 U.S.C. 1681u(a)(2000 ed.).

[69] National Security Letters: The Need for Greater Accountability and Oversight: Hearing Before the Senate Comm. on the Judiciary, 110th Cong., 2d sess. (2008)(testimony of Michael J. Woods, former Chief of the FBI's National Security Law Unit), available on Oct. 23, 2009 at [http://judiciary.senate.gov/pdf/08-04-23WoodsTestimony.pdf].

[70] P.L. 109-177, 120 Stat. 192 (2006), and P.L. 109-178, 120 Stat. 278 (2006), respectively.

[71] Depending upon one's perspective these provisions may be described as nondisclosure provisions, secrecy provisions, or gag order provisions. The descriptions are used interchangeably without any intended connotations in this report.

[72] 18 U.S.C. 2709((c), 12 U.S.C. 3414(a)(5)(D), 15 U.S.C. 1681u(d).

The impact might be less significant that would at first appear. By and large, 18 U.S.C. 3511 governs judicial review of NSL nondisclosure requirements. When implemented as required by the Second Circuit's decision in *John Doe, Inc. v. Mukasey,* 549 U.S. 861 (2d Cir. 2008), and at the election of the recipient, the government has the burden of persuading the court of the validity of the gag order under the same standards as found in the expired portions of the NSL statutes. Although each of the legislative proposals would amend section 3511, explicitly or implicitly, they each reinforce rather than erode the recipient protections of section 3511 as discussed *infra*.

Section 627, the NSL statute created in the USA PATRIOT Act, is arguably the most sweeping of the NSL statutes. It offers the most extensive array of information (all information pertaining to a consumer held by a consumer credit reporting agency) to the widest range of requesters (any federal agency "authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis relating to, international terrorism").[73] Its repeal might be seen to facilitate oversight, since it would centralize authority to issue NSLs in the FBI (other than in the case of employee security investigations under the National Security Act). Moreover, the Justice Department IG reported that both the FBI and consumer reporting agencies have experienced difficulty distinguishing between authority under 1681u and 1681v.[74]

In contrast, the National Security Act NSL statute, left unamended by the USA PATRIOT Act is arguably the least intrusive. It reaches only information pertaining to federal employees who have consented to their disclosure.[75]

Nondisclosure

Each of the NSL statutes has a nondisclosure provision.[76] They state that the issuing agency may prohibit recipients from disclosing the request – to anyone other than their attorney and those necessary to comply with the request, ever.[77] In order to activate the authority, agency officials must certify that disclosure may endanger national security, endanger individual safety, or may interfere with diplomatic relations or with a criminal, counterintelligence, or counterterrorism investigation.[78]

---

[73] 15 U.S.C. 1681v(a). Such agencies would presumably include at a minimum those agencies who are members of the "intelligence community," see e.g., 50 U.S.C. 401a(4)("The term 'intelligence community' includes the following: (A) The Office of the Director of National Intelligence. (B) The Central Intelligence Agency. (C) The National Security Agency. (D) The Defense Intelligence Agency. (E) The National Geospatial-Intelligence Agency. (F) The National Reconnaissance Office. (G) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs. (H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, and the Department of Energy. (I) The Bureau of Intelligence and Research of the Department of State. (J) The Office of Intelligence and Analysis of the Department of the Treasury. (K) The elements of the Department of Homeland Security concerned with the analysis of intelligence information, including the Office of Intelligence of the Coast Guard. (L) Such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community"). Admittedly, section 1681v only identifies those who may invoke NSL authority, not necessarily those who have or will exercise that authority.

[74] *IG Report I*, at 80-1, 125; *IG Report II*, at 29-30.

[75] 50 U.S.C. 436(a)(3)(A).

[76] 12 U.S.C. 3414(a)(5)(D); 18 U.S.C. 2709(c); 15 U.S.C. 1681u(d); 15 U.S.C. 1681v(c); 50 U.S.C. 436(b).

[77] Id.

[78] Id.

A federal district court may modify or set aside a NSL secrecy requirement on the petition of a recipient, if it concludes that there is no reason to believe that disclosure might result in any such danger or interference.[79] If the petition for review is filed more than a year after issuance of the NSL, the agency must either terminate the gag order or recertify the need for its continuation.[80] There is no explicit provision for disclosure to the party to whom the information pertains.

The Second Circuit in *John Doe, Inc. v. Mukasey* held that these provisions only survive First Amendment scrutiny if the agency petitions for judicial review and convinces the court that the agency proposed order is narrowly crafted to meet to the statutorily identified adverse consequences of disclosure.[81]

The Nadler, Conyers, Feingold and Leahy bills would each modify the statutory provisions governing the issuance and judicial review of NSL nondisclosure orders. The Conyers, Feingold and Leahy bills would codify a procedure comparable in many respects to that which the Second Circuit identified as constitutionally acceptable. Under all three bills, the agency issuing the NSL would make the initial determination of whether to include a nondisclosure provision in the NSL and that determination would be subject to judicial review.[82] The Nadler bill uses a different approach to meet the Second Circuit requirement that the government seek and justify judicial approval for a nondisclosure order. Under the Nadler bill, recipients would be under a disclosure ban for 30 days during which the agency might apply to the court to issue a nondisclosure order.[83]

The Leahy and Conyers bills would leave unchanged the concerns a requesting official might rely upon in order to impose a nondisclosure order: reason to believe disclosure may endanger national security or individual safety or interfere with diplomatic relations or a criminal, counterterrorism, or counterintelligence investigation (but in the Conyers bill the court would have to find that disclosure would – rather than might – result in one or more of the adverse consequences).[84] The Nadler and Feingold bills would adopt a higher threshold and would establish a narrower range of adverse consequences necessary to justify nondisclosure: reason to believe disclosure "will" (rather than "may") result in a danger to personal safety; flight from prosecution; destruction or tampering with evidence; witness intimidation; a serious danger to national security by tipping off the foreign agent who is the target of the investigation, or his associates, or the foreign power that is the agent's principal; or (only in the case of the Feingold bill) interfere with diplomatic relations.[85]

The Nadler and Feingold bills would adopt a higher threshold as well and would establish a narrower range of adverse consequences necessary to justify nondisclosure: reason to believe disclosure "will" (rather than "may") result in a danger to personal safety; flight from

[79] 18 U.S.C. 3511(b)(1), (2).

[80] 18 U.S.C. 3511(b)(1), (3).

[81] 549 F.3d 861, 883 (2d Cir. 2008).

[82] H.R. 3845, §207; proposed 18 U.S.C. 3511(b). S. 1686, §101; proposed 18 U.S.C. 2709(c); 12 U.S.C. 3414((b); 15 U.S.C. 1681u(b).

[83] H.R. 3845, §207, proposed 18 U.S.C. 3511(b).

[84] S. 1692, §5; proposed 18 U.S.C. 2709(c)(1)(B); 15 U.S.C. 1681u(d)(1)(B); 15 U.S.C. 1681v(c)(1)(B); 12 U.S.C. 3414(a)(5)(D)(i)(II); 50 U.S.C. 436(b)(1)(B). H.R. 3845, §207, proposed 18 U.S.C. 3511(b).

[85] H.R. 1800, §3(d)(5). Most of the amendments in H.R. 1800 and S. 1686 would not apply to 50 U.S.C. 436. S. 1686, §101; proposed 18 U. 18 U.S.C. 2709(c)(1)(B); 15 U.S.C. 1681u(b); 12 U.S.C. 3414(b). S. 1686 would repeal 15 U.S.C. 1681v.

prosecution; destruction or tampering with evidence; witness intimidation; a serious danger to national security by tipping off the foreign agent who is the target of the investigation, or his associates, or the foreign power that is the agent's principal; or (only in the case of the Feingold bill) interfere with diplomatic relations.[86]

In all four bills, the government would bear the burden of petitioning for and securing U.S. district court approval of a nondisclosure provision. In the Nadler bill, the recipient would be subject to a preliminary 30 day nondisclosure requirement during which the issuing agency might seek a court nondisclosure order.[87] In the Feingold bill, should the agency determine that nondisclosure is appropriate it would inform the recipient that he had 21 days to ask for judicial review.[88] Those who elect not to request judicial review would be bound by the nondisclosure requirement for not more than a year.[89] In the case of those who request judicial review, the agency would have 21 days to petition the court for review.[90] In the Leahy and Conyers bills, the agency would notify the recipient of the right to judicial review and petition for review within 30 days of a recipient's request for judicial review.[91]

All four bills would require that the agency's application for judicial approval or review include a statement of facts giving reason to believe that disclosure would (or might in the case of the Leahy and Conyers bills) result in one of the statutory list of adverse consequences – (A) in the Leahy and Conyers bills, endanger national security or individual safety or interfere with diplomatic relations or with a criminal, counterterrorism, or counterintelligence investigation; or (B) in the Nadler and Feingold bills, endanger personal safety; flight from prosecution; destruction or tampering with evidence; witness intimidation; a serious danger to national security by tipping off the foreign agent who is the target of the investigation, or his associates, or the foreign power that is the agent's principal; or (only in the case of the Feingold bill) interfere with diplomatic relations.[92]

The Feingold bill would compel applicants to explain how the adverse consequences relate to the investigation in which NSL is sought and how the secrecy order is narrowly crafted to counter the possibility of those adverse consequences.[93] In addition, the Feingold bill would require that agency applicants recommend when the secrecy order should expire.[94]

---

[86] H.R. 1800, §3(d)(5). Most of the amendments in H.R. 1800 and S. 1686 would not apply to 50 U.S.C. 436. S. 1686, §101; proposed 18 U. 18 U.S.C. 2709(c)(1)(B); 15 U.S.C. 1681u(b); 12 U.S.C. 3414(b). S. 1686 would repeal 15 U.S.C. 1681v.

[87] H.R. 1800, §3(d).

[88] S. 1686, §§101, 102; proposed 18 U.S.C. 2709(c)(4); 15 U.S.C. 1681u(b); 12 U.S.C. 3414(b); 18 U.S.C. 3511(b). S. 1686 would repeal 15 U.S.C. 1681v, and most of the amendments in S. 1686 would not apply to 50 U.S.C. 436. S. 1692, §5; proposed 18 U.S.C. 2709(c)(4); 15 U.S.C. 1681u(d)(4); 15 U.S.C. 1681v(c)(4); 12 U.S.C. 3414(a)(5)(D)(iv); 50 U.S.C. 436(b)(4); 18 U.S.C. 3511(b).

[89] S. 1686, §101; proposed 18 U.S.C. 2709(c)(1); 15 U.S.C. 1681u(b); 12 U.S.C. 3414(b). S. 1686 would repeal 15 U.S.C. 1681v, and most of the amendments in S. 1686 would not apply to 50 U.S.C. 436. S. 1692, §5; proposed 18 U.S.C. 2709(c)(1); 15 U.S.C. 1681u(d)(1); 15 U.S.C. 1681v(c)(4); 12 U.S.C. 3414(a)(5)(D)(iv); 50 U.S.C. 436(b)(4); 18 U.S.C. 3511(b).

[90] S. 1686, §102; proposed 18 U.S.C. 3511(b)(1). S. 1692, §6(b), proposed 18 U.S.C. 3511(b)(1).

[91] S. 1692, §6(b); proposed 18 U.S.C. 3511(b)(1). H.R. 3845, §207, proposed 18 U.S.C. 3511(b)(1).

[92] H.R. 1800, §3(d). H.R. 3845, §207, proposed 18 US.C. 3511(b)(2). S. 1686, §102; proposed 18 U.S.C. 3511(b)(2). S. 1692, §6(b); proposed 18 U.S.C. 3511(b)(2).

[93] S. 1686, §102; proposed 18 U.S.C. 3511(b)(2).

[94] S. 1686, §102; proposed 18 U.S.C. 3511(b)(2). S. 1692, §6(b); proposed 18 U.S.C. 3511(b)(2).

Should the court feel the agency has met its burden, it would be authorized to approve the requested secrecy order. The Feingold bill limits the order to no more than a year; the Nadler and Conyers bills to no more than 180 days.[95] Renewals would be available under the same conditions and with the maximum duration as in the original.[96] Unlike the other bills, the Leahy bill has no such explicit provision for maximum duration of a gag order, and unlike existing law, it has no explicit provision to allow a recipient to petition for judicial review after the passage of time. On the other hand, it places no express time limit on the recipient's right to judicial review nor upon the court's jurisdiction over the question; it states only that the recipient has a right to judicial review of the order, that the recipient must notify the agency of any desire for judicial review, and that the agency must be petition the court for review within 30 days of receiving a recipient's request.[97]

Judicial Review of NSL Itself

Existing law permits the recipient of a NSL to petition the U.S. district court to modify it or set aside under the same grounds as a grand jury subpoena might be quashed or modified or if it is otherwise unlawful.[98] The Conyers, Feingold and Leahy bills would not change existing law here, although they would provide that a NSL include a statement informing the recipient of his right to seek judicial review and of the procedures for doing so.[99] The Nadler bill contains a provision which appears to be designed to replace existing law, although the bill would neither repeal nor expressly amend the current provision. The Nadler proposal would allow a recipient to petition the U.S. district court to modify or set aside the NSL for failure to comply with the statutory requirements associated with the issuance of NSL or based "upon any constitutional or other legal right or privilege" of the recipient.[100]

Issuance and Content

The NSL statutes now authorize the NSLs upon certification that the information is sought for, or is relevant to, various national security investigations.[101] The Nadler and Conyers bills would require certification of specific and articulable facts supporting a belief that the information pertains to a foreign power or one of its agents.[102] The Feingold bill would require certification of specific and articulable facts supporting a belief that the information pertains to (i) a suspected

[95] H.R. 1800, §3(d). H.R. 3845, §207, proposed 18 U.S.C. 3511(b)(1). S. 1686, §102; proposed 18 U.S.C. 3511(b)(1).

[96] H.R. 1800, §3(d). H.R. 3845, §207, proposed 18 U.S.C. 3511(b)(4). S. 1686, §102; proposed 18 U.S.C. 3511(b)(4).

[97] S. 1692, §§5, 6(b); proposed 18 U.S.C. 3511(b)(1) 18 U.S.C. 2709(c)(3); 12 U.S.C. 3414(a)(5)(D)(iii); 15 U.S.C. 1681u(d)(3); 15 U.S.C. 1681v(d)(3), 50 U.S.C. 436(b)(3). Each of the revised NSL statutes would require an agency to terminate a no longer necessary nondisclosure order upon a request for judicial review which seems to confirm that the Leahy bill contemplates recipient requests for judicial review after the passage of time. S. 1692, §5; proposed 18 U.S.C. 2709(c)(4); 12 U.S.C. 3414(a)(5)(D)(iv); 15 U.S.C. 1681u(d)(4); 15 U.S.C. 1681v(d)(4), 50 U.S.C. 436(b)(4).

[98] 18 U.S.C. 3511(a).

[99] Id.

[100] H.R. 1800, §3(e)(1).

[101] 18 U.S.C. 2709 (relevant to an investigation to protect against international terrorism or clandestine intelligence activities); 12 U.S.C. 3414(5)(A)(sought for foreign counterintelligence purposes); 15 U.S.C. 1681u (a)(sought for an investigation to protect against international terrorism or clandestine intelligence activities); 15 U.S.C. 1681v(a) (necessary for an agency's investigation, activity, or analysis relating to international terrorism); 50 U.S.C. 436(sought for an inquiry or investigation relating to agency employees with access to classified information).

[102] H.R. 1800, §3(a). H.R. 3845, §204.

agent of a foreign power or the subject of a national security investigation, (ii) an individual in contact with or directly linked to such an individual, or (iii) the activities of such an individual when the activities are the subject of a national security investigation and the NSL is the least intrusive means to identifying persons involved.[103] The Leahy bill has no comparable provision, but it would insist upon a written statement of facts supporting the conclusion that the information sought is relevant to the investigation for which it is sought.[104]

Both the Nadler bill and the Feingold bill would prohibit NSL demands that would be considered unreasonable or privileged, if sought under a grand jury subpoena duces tecum.[105] The Conyers and Leahy bills have no comparable provisions.

Minimization Requirements

In a general sense "minimization" refers to limitations on what information is acquired; how it is acquired; how it is maintained; who has access to it within the capturing agency and under what circumstances; to whom and under what circumstances it is disclosed beyond the capturing agency; how long it is preserved; and when and under what circumstances it is expunged. Minimization standards are drawn with an eye to the purposes for which information is acquired; the authority under which it is acquired; the legitimate interests which may be affected by its acquisition, use, or disclosure; and the governmental interests served by its acquisition, maintenance, use, and disclosure.

Minimization standards ordinarily reinforce statutory and regulatory limitations that attend the use of possibly invasive means of acquiring information. For example, the Foreign Intelligence Surveillance Act (FISA) provides fairly rigorous statutory procedures that must be honored before electronic surveillance or physical searches may be authorized in a national security context, 50 U.S.C. 1801-1829. It also supplies statutory conditions under which information acquired using those techniques may be used, e.g., 50 U.S.C. 1806, and both judicial and legislative oversights procedures, e.g., 50 U.S.C. 1805, 1808. As an additional safeguard, it also calls for the creation and implementation of minimization procedures to protect private information relating to Americans consistent with the U.S. foreign intelligence interests, *e.g.*, 50 U.S.C. 1801(h), 1802(a)(2).[106]

---

[103] S. 1686, §101; proposed 18 U.S.C. 2709(b)(1); 12 U.S.C. 3414(b); 1681u(b). S. 1686 would repeal 15 U.S.C. 1681v, and most of the amendments in S. 1686 would not apply to 50 U.S.C. 436.

[104] S. 1692, §7; proposed 18 U.S.C. 2709(b)(1); 15 U.S.C. 1681u(b); 15 U.S.C. 1681v(a); 12 U.S.C. 3414(a)(5)(A); 50 U.S.C. 436(a)(3).

[105] H.R. 1800, §3(c). S. 1686, §101; proposed 18 U.S.C. 2709(b)(3); 12 U.S.C. 3414(b); 15 U.S.C. 1681u(b). S. 1686 would repeal 15 U.S.C. 1681v, and most of the amendments in S. 1686 would not apply to 50 U.S.C. 436.

[106] 50 U.S.C. 1801(h)("'Minimization procedures', with respect to electronic surveillance, means – (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any (continued...)

Section 119(f) of the USA PATRIOT Improvement and Reauthorization Act directed the Attorney General and the Director of National Intelligence to report to the Congressional intelligence and judiciary committees on the feasibility of NSL minimization procedures "to ensure the protection of the constitutional rights of Untied States persons."[107] The Inspector General's reports noted the need for minimization standards or their regulatory equivalent:

> In our first NSL report, the OIG noted the proviso in the Attorney General's NSI Guidelines that national security investigations should use the "least intrusive collection techniques feasible" to carry out the investigations. The OIG reported that we found no clear guidance on how Special Agents should reconcile the Attorney General guidelines' limitations with the expansive authority provided in the NSL statutes. Our concerns over the lack of formal guidance were magnified because of the volume of NSLs generated by the FBI each year and because the information collected is retained for long periods in databases available to many authorized law enforcement personnel.[108]

The Justice Department convened a working group to study and make recommendations concerning possible NSL minimization standards in response to its statutory obligation and the Inspector General's initial report.[109] The working group's proposals have yet to be finalized and the Inspector General recently testified that "final guidance is needed and overdue."[110]

Each of the bills has minimization components. Some take the form of statutory limitations and others instructions for Justice Department guidelines. The Leahy and Feingold bills would direct the Attorney General to promulgate minimization procedures within 180 days with features comparable to the FISA definition in 50 U.S.C. 1801(h): procedures that are calculated, consistent with U.S. needs for foreign intelligence information, to minimize the capture and retention of private information (information not publicly available) relating to a U.S. person (and to ban its retention); procedures that preclude the disclosure of private information relating to a U.S. person (that is not foreign intelligence information) that identifies the person, unless necessary to appreciate its significance; and procedures that permit evidence of a crime to be retained and disclosed.[111] The Feingold bill would also insist that the procedures call for the return or

(...continued)

communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person").

[107] P.L. 109-177, 120 Stat. 220 (2006).

[108] *IG Report II*, at 64; see also *id.* at 68 n.41 ("In general, information related to intelligence investigations is retained in the FBI's files (either in the paper case file or in the FBI's electronic systems) for 30 years after a case is closed, and information related to criminal investigations is retained for 20 years after a case is closed. After that time, the case information is reviewed, and information that is identified for permanent retention is transferred to the National Archives and Records Administration (NARA) for storage. Any cases not meeting the criteria for permanent retention and transfer to the NARA are destroyed"); *IG Report I*, at 110 ("neither the Attorney General's NSI Guidelines nor internal FBI policies require the purging of information derived from NSLs in FBI databases, regardless of the outcome of the investigation. Thus, once information is obtained in response to a national security letter, it is indefinitely retained and retrievable by the many authorized personnel who have access to various FBI databases").

[109] IG Report II, at 64.

[110] Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security: Hearing Before the Senate Comm. on the Judiciary, 111th Cong., 1st sess. (2009)(statement of Inspector General Glenn A. Fine).

[111] S. 1686, §101; proposed 18 U.S.C. 2709(d); 12 U.S.C. 3414(b); 15 U.S.C. 1681u(b). S. 1692, §12.

destruction of information acquired outside the scope of the NSL or in a manner that fails to comply with the NSL statute.[112]

The Nadler and Conyers bills would give the Attorney General 90 days to promulgate minimization procedures that are calculated to minimize the capture and retention of private information (information not publicly available) relating to a U.S. person (and to ban its dissemination).[113] The additional requirements would focus on procedures for the return or destruction of information that does not reflect the activity of an agent of a foreign power; that is superfluous; or that exceeds the bounds of the original NSL request.[114]

In provisions modeled after those in FISA, the Nadler and Feingold bills would also add explicit provisions describing some of the circumstances under which NSL generated information might be disclosed. They would:

- prohibit disclosure except for lawful purposes and in compliance with minimization procedures;
- require a statement of origin and of Attorney General approval when used in criminal proceedings;
- when the information is to be used in federal proceedings, direct that the person to whom the information relates and the tribunal be informed beforehand of the information's source;
- when the information is to be used in state proceedings, direct that the person to whom the information relates, the tribunal, and the Attorney General be informed beforehand of the information's source and intended use;
- when the information is to be used in either state or federal proceedings, afford the person to whom the information relates an opportunity to move for suppression based on the NSL statute, the Constitution, or other laws of the United States;
- authorize the U.S. district court to order suppression should it find that due process so requires or that the NSL was not issued in compliance with the NSL statute, the Constitution, or other laws of the United States; and
- make binding the U.S. district court's suppression decisions except for federal appellate purposes.[115]

The Conyers bill would require the Attorney General's prior approval before NSL information could be used in a criminal proceeding.[116]

The Feingold bill also includes a "least intrusive means" section.[117] The current Attorney General's guidelines governing FBI intelligence investigations in this country state that the FBI

[112] S. 1686, §101; proposed 18 U.S.C. 2709(d); 12 U.S.C. 3414(b); 15 U.S.C. 1681u(b).

[113] H.R. 1800, §6. H.R. 3845, §208.

[114] Id.

[115] H.R. 1800, §3(f). S. 1686, §101; proposed 18 U.S.C. 2709(f); 12 U.S.C. 3414(b); 15 U.S.C. 1681u(b). S. 1686 would repeal 15 U.S.C. 1681v, and most of the amendments in S. 1686 would not apply to 50 U.S.C. 436.

[116] H.R. 3845, §206.

investigations should use the "least intrusive method feasible" in light of the circumstances.[118] The Feingold bill would establish a statutory least intrusive means NSL standard and would require recourse to other sources before the issuance of a NSL directed to a bookstore or library.[119]

Emergency Practices

The IG's first report indicated that in a number of instances the FBI had used "exigent letters" and "certificate letters" rather than NSL statutory authority to "circumvent" NSL requirements.[120] Although they had not relied upon it, the FBI asserted that in some of those instances they might have invoked the voluntary disclosure provisions of 18 U.S.C. 2702.[121]

Section 2702 authorizes communications providers to supply "a governmental entity" with customer communications content and records, "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications [or information] relating to the emergency."[122]

The Nadler and Feingold bills would amend section 2702 to limit the exception to where the risk of death or serious injury is imminent or immediate.[123] The Feingold bill would also add a provision to the Right to Financial Privacy Act to allow a comparable disclosure of customer records by financial institutions under similar circumstances.[124] The change seems intended to make clear that there are no implicit emergency grounds for disclosure of such records.

Reports and Audits

Some of the NSL statutes provide for periodic reports to various Congressional committees.[125] In addition, the USA PATRIOT Improvement and Reauthorization Act instructed the Attorney General to prepare, in unclassified form, an annual report to Congress on the number of NSLs issued in the previous year.[126] The same legislation directed the Inspector General of the Department of Justice to audit and report on the use of NSL authority for calendar years 2002 through 2006.[127]

The Nadler, Feingold and Leahy bills would each expand the annual statistical report to include a breakdown of the number of NSLs issued concerning U.S. persons, those who are not U.S.

(...continued)

[117] S. 1686, §106.

[118] *The Attorney General's Guidelines for Domestic FBI Operations*, at 12-3 (Sept. 29, 2008), available on Oct. 26, 2009 at http://www.justice.gov/ag/readingroom/guidelines.pdf.

[119] S. 1686, §106.

[120] *IG Report I*, 92-8, 115-18.

[121] *Id.* at 94-5.

[122] 18 U.S.C. 2702(b)(8), (c)(4).

[123] H.R. 1800, §7. S. 1686, §105.

[124] S. 1686, §105(b).

[125] 18 U.S.C. 2709(e); 15 U.S.C. 1681u(h); 15 U.S.C. 1681v(f).

[126] P.L. 109-177, §118, 120 Stat. 217 (2006), 18 U.S.C. 3511 note.

[127] P.L. 109-177, §119, 120 Stat. 219 (2006).

persons, the targets of national security investigation, and those who are not the target of a national security investigation.[128] The Leahy and Conyers bills would call for Inspector General audits and reports covering the years 2007 through 2009 and annual audits and reports for calendar years 2010 and 2011(as well as 2012 and 2013 under the Conyers bill).[129]

[128] H.R. 1800, §6(c). S. 1686, §104. S. 1692, §8.

[129] S. 1692, §10. H.R. 3845, §105(b).

Table 2. Chart of Proposed NSL Amendments: H.R. 3845, H.R. 1800, S. 1686, and S. 1692

Current Law	H.R. 3845 (Conyers)	H.R. 1800 (Nadler)	S. 1686 (Feingold)	S. 1692 (Leahy)
Sunset				
NSL statutes have no expiration date	Effective Dec. 3, 2013, NSL statutes revert to pre-USA PATRIOT Act versions and 15 USC 1681v is thereby repealed (§202)	After 5 years, NSL statutes (except 50 USC 436) revert to pre-USA PATRIOT Act versions and 15 USC 1681v is thereby repealed (§5(a))	Repeals 15 USC 1681v (§101(c)(2))	Effective Dec. 31, 2013, NSL statutes revert to pre-USA PATRIOT Act versions and 15 USC 1681v is repealed (§2(c))
Gag orders:				
Recipient may seek judicial review, 18 USC 3511 (2d Cir. valid only if agency secures court approval when recipient requests (549 F.3d 861)	Upon recipient request, agency has 30 days to seek a court order of < 180 days; renewals of < 180 days (§207)	Agency issued (up to 30 days) pending US district court order of <180 days; renewals of <180 days (§3(d))	Agency issued (recipient may request jud. rev. w/i 21 days); upon request, agency has 21 days to seek court order (orders limited to 1 year; renewals for 1 year possible) (§102)	Agency issued (recipient may request jud. rev.); upon request, agency has 30 days to seek a court order (no statutory max. duration); bill appears to contemplate continuous right to request review (§§5, 6(b))
Grounds				
Agency cert. & ct. approval if any reason to believe disclosure might: endanger US national security/individual safety; or interfere w/ diplomatic relations or w/ a criminal, counterintell, or counterterr. investigation (18 USC 3511)	Agency certification & court approval granted if there is any reason to believe disclosure might(agency)/will(ct): endanger US national security or individual safety; or interfere with diplomatic relations or with a criminal, counterintelligence, or counterterrorism investigation (§207)	Agency application stating specific and articulable facts for believe disclosure will result in : danger to individual safety; flight to avoid prosecution, destruction or tampering with evidence, or danger to national security (by tipping off the target of the investigation, his associates or foreign principal) (§3(d)(5),(d)(6))	Same as H.R. 1800 except adds interference with diplomatic relations to the list of adverse consequences that may justify a gag order (§101 – prop. 18 USC 2709(c), 12 USC 3414(b), 15 USC 1681u(b))	Agency statement of facts and court determination that disclosure will result in: danger to US national security or individual safety; or interfere with diplomatic relations or with a criminal, counterintelligence, or counterterrorism investigation (§6(b))
NSL: Grounds				
Relevancy to various national security investigations (e.g., 18 USC 2709(b))	Specific/articulable facts showing info pertains to a foreign power/agent in separate letter for the files (§204)	Specific and articulable facts exist showing info pertains to a foreign power/agent (§3(a))	Specific and articulable facts showing info pertains to (i) suspected foreign power agent/individual subject of a national security investigation; (ii) individual in contact with/directly linked to (i); or (iii) activities of a suspected for. power agent (if activities are under national security investigation and NSL is least intrusive means)(§101)	Relevancy to various national security investigations and agency retains writtenstatement specific factual basis for conclusion (§7)

Current Law	H.R. 3845 (Conyers)	H.R. 1800 (Nadler)	S. 1686 (Feingold)	S. 1692 (Leahy)
Minimization				
DoJ is finalizing minimization standards	Directs DoJ to issue standards w/i 90 days covering (1) minimum capture/keep (no passing on) nonpublic info in re US persons (consistent w/ US for. intell. needs); (2) burn ASAP info in re US person not a for. power agent, info in excess of NSL, & superfluous info (§208)	Same as H.R. 3845 (§6)	Directs DoJ to issue standards w/i 180 days covering (1) minimum capture/keep (no passing on) nonpublic info in re US persons (consistent w/ US for. intell. needs); (2) passing on non public info in re US person (if not for. intell. info) that id.s person (unless needed for context); permit keep/pass on evidence of crime (§101)	Same as S. 1686 (§12)
	Requires AG notification before use of NSL info in criminal proceedings (§206)	Adapts FISA-like use-in-official-proceeding features (§3(f))	Same as H.R. 1800 (§101)	
Audits & Reports				
Audits				
DoJ IG audited and reported on FBI NSL use for 2003, 2004, 2005 & 2006 (120 Stat. 219)	Requires DoJ IG audits and reports on FBI NSL use for 2007-2009 and annual audits/repts for, 2010, 2011, 2012 & 2013 (§105(b))			Requires DoJ IG audit and reports covering the years 2007, 2008 and 2009, and annual reports for 2010 and 2011 (§10(b))
Reports				
Requires annual DoJ report to Congress in unclassified form on total number of NSL requests in re US persons (120 Stat. 218)		Requires semiannual DoJ report in unclassified form on: the total number of NSL requests under each NSL statute, for procedures and any changes to them; summary of any judicial challenges; the extent to which NSLs aided investigations and prosecutions (§6(c)	Except with regard to subscriber information under 18 USC 2709, requires the annual report to include the nubmer NSL requests concerning US persons, non-US persons, persons who were the subject of national security investigations, and those who were not (§104	Same as S. 1686
Emergency Practices				
Communications providers may disclose the content and records of customer communications in threat of death or serious physical injury cases (18 USC		Limit such voluntary disclosures to threats of imminent or immediate death or serious injury cases (§7	Same as H.R. 1800(§105(a))	

Current Law	H.R. 3845 (Conyers)	H.R. 1800 (Nadler)	S. 1686 (Feingold)	S. 1692 (Leahy)
2702((b)(8), (c)(4))			Permits financial institutions to disclose customer financial information to government authorities in cases of a threat of immediate death or serious physical injury (§1105(b))	

Text of NSL Statutes on October 25, 2001 and Now (emphasis added)

12 U.S.C. 3414(a)(5) (on October 25, 2001)

* * *

(a) . . . .
(5)(A) Financial institutions, and officers, employees, and agents thereof, shall comply with a request for a customer's or entity's financial records made pursuant to this subsection by the Federal Bureau of Investigation when the Director of the Federal Bureau of Investigation (or the Director's designee) certifies in writing to the financial institution that such records are sought for foreign counter intelligence purposes *and that there are specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or the agents of a foreign power as defined in section 1801 of title 50.*
(B) The Federal Bureau of Investigation may disseminate information obtained pursuant to this paragraph 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.
(C) On a semiannual basis the Attorney General 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 pursuant to this paragraph.
(D) No financial institution, or officer, employee, or agent of such institution, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to a customer's or entity's financial records under this paragraph.

12 U.S.C. 3414(a)(5) (now)

* * *

(a) . . .
(5)(A) Financial institutions, and officers, employees, and agents thereof, shall comply with a request for a customer's or entity's financial records made pursuant to this subsection by the Federal Bureau of Investigation when the Director of the Federal Bureau of Investigation (or the Director's 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 in writing to the financial institution that such records are sought for foreign counter intelligence purposes *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.*
(B) The Federal Bureau of Investigation may disseminate information obtained pursuant to this paragraph 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.
(C) On the dates provided in section 415b of Title 50, the Attorney General shall fully inform the

congressional intelligence committees (as defined in section 401a of Title 50) concerning all requests made pursuant to this paragraph.

(D) Prohibition of certain disclosure. –

(i) *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 financial institution, or officer, employee, or agent of such institution, 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 a customer's or entity's financial records under subparagraph (A).

(ii) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under clause (i).

(iii) 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 persons of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under clause (i).

(iv) 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 for financial records under subparagraph (A).

15 U.S.C. 1681u(a), (b)(on October 25, 2001).

(a) Identity of financial institutions

Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions (as that term is defined in section 3401 of Title 12) at which a consumer maintains or has maintained an account, to the extent that information is in the files of the agency, when presented with a written request for that information, signed by the Director of the Federal Bureau of Investigation, or the Director's designee, which certifies compliance with this section. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that –

(1)such information is necessary for the conduct of an authorized foreign counterintelligence investigation; and

(2) there are specific and articulable facts giving reason to believe that the consumer –

(A) is a foreign power (as defined in section 1801 of title 50) or a person who is not a United States person (as defined in such section 1801 of title 50) and is an official of a foreign power; or

(B) is an agent of a foreign power and is engaging or has engaged in an act of international terrorism (as that term is defined in section 1801(c) of title 50) or clandestine intelligence activities that involve or may involve a violation of criminal statutes of the United States.

(b) Identifying information
Notwithstanding the provisions of section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request, signed by the Director or the Director's designee, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that –

(1) such information is necessary to the conduct of an authorized counterintelligence investigation; and

(2) there is information giving reason to believe that the consumer has been, or is about to be, in contact with a foreign power or an agent of a foreign power (as defined in section 1801 of title 50).

* * *

15 U.S.C. 1681u(a), (b)(now).

(a) Identity of financial institutions
Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions (as that term is defined in section 3401 of Title 12) at which a consumer maintains or has maintained an account, to the extent that information is in the files of the agency, when presented with a written request for that information, signed by the Director of the Federal Bureau of Investigation, or the Director's designee *in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director*, which certifies compliance with this section. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing, that *such information is sought for the conduct of 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.*

(b) Identifying information
Notwithstanding the provisions of section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request, signed by the Director or the Director's designee *in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director*, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that *such information is sought for the conduct of 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*.

* * *

18 U.S.C. 2709 (as of October 25, 2001)

(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, 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 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 investigation to foreign counterintelligence investigation; and

(*B) there are specific and 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 communications 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 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.

(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.

(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.

18 U.S.C. 2709 (now)

(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 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, 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*.

(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, 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 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.

15 U.S.C. 1681v (as of October 25, 2001)

NONE. This section was created by the USA PATRIOT Act, effective October 26, 2001.

15 U.S.C. 1681v (now)

(a) Disclosure
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.

(b) Form of certification
The certification described in subsection (a) of this section shall be signed by a supervisory official designated by the head of a Federal agency or an officer of a Federal agency whose appointment to office is required to be made by the President, by and with the advice and consent of the Senate.

(c) Confidentiality
(1) If the head of a government agency authorized to conduct investigations of intelligence or counterintelligence activities or analysis related to international terrorism, or his designee, 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 consumer

reporting agency or officer, employee, or agent of such consumer reporting agency, 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), or specify in any consumer report, that a government agency has sought or obtained access to information under subsection (a) of 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 any attorney to obtain legal advice or legal assistance with respect to the request shall inform such persons 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 authorized government agency, any person making or intending to make a disclosure under this section shall identify to the requesting official of the authorized government agency 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 requesting official 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 for information under subsection (a) of this section.

(d) Rule of construction
Nothing in section 1681u of this title shall be construed to limit the authority of the Director of the Federal Bureau of Investigation under this section.

(e) Safe harbor
Notwithstanding any other provision of this subchapter, any consumer reporting agency or agent or employee thereof making disclosure of consumer reports or other information pursuant to this section in good-faith reliance upon a certification of a government agency pursuant to the provisions of this section shall not be liable to any person for such disclosure under this subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

(f) Reports to Congress
(1) On a semi-annual basis, the Attorney General shall fully inform the Committee on the Judiciary, the Committee on Financial Services, and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary, the Committee on Banking, Housing, and Urban Affairs, and the Select Committee on Intelligence of the Senate concerning all requests made pursuant to subsection (a) of this section.
(2) In the case of the semiannual reports required to be submitted under paragraph (1) to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, the submittal dates for such reports shall be as provided in section 415b of Title 50.

50 U.S.C. 436 (as of October 25, 2001)

(a) Generally
(1) Any authorized investigative agency may request from any financial agency, financial institution, or holding company, or from any consumer reporting agency, such financial records, other financial information, and consumer reports as may be necessary in order to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination. Any authorized investigative agency may also request records maintained by any commercial

entity within the United States pertaining to travel by an employee in the executive branch of Government outside the United States.

(2) Requests may be made under this section where –

(A) the records sought pertain to a person who is or was an employee in the executive branch of Government required by the President in an Executive order or regulation, as a condition of access to classified information, to provide consent, during a background investigation and for such time as access to the information is maintained, and for a period of not more than three years thereafter, permitting access to financial records, other financial information, consumer reports, and travel records; and

(B)(i) there are reasonable grounds to believe, based on credible information, that the person is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(ii) information the employing agency deems credible indicates the person has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other information known to the agency; or

(iii) circumstances indicate the person had the capability and opportunity to disclose classified information which is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Each such request –

(A) shall be accompanied by a written certification signed by the department or agency head or deputy department or agency head concerned, or by a senior official designated for this purpose by the department or agency head concerned (whose rank shall be no lower than Assistant Secretary or Assistant Director), and shall certify that –

(i) the person concerned is or was an employee within the meaning of paragraph (2)(A);

(ii) the request is being made pursuant to an authorized inquiry or investigation and is authorized under this section; and

(iii) the records or information to be reviewed are records or information which the employee has previously agreed to make available to the authorized investigative agency for review;

(B) shall contain a copy of the agreement referred to in subparagraph (A)(iii);

(C) shall identify specifically or by category the records or information to be reviewed; and

(D) shall inform the recipient of the request of the prohibition described in subsection (b) of this section.

(b) *Disclosure of requests*

Notwithstanding any other provision of law, no governmental or private entity, or officer, employee, or agent of such entity, may disclose to any person that such entity has received or satisfied a request made by an authorized investigative agency under this section.

* * *

50 U.S.C. 436 (now)

(a) Generally

(1) Any authorized investigative agency may request from any financial agency, financial institution, or holding company, or from any consumer reporting agency, such financial records, other financial information, and consumer reports as may be necessary in order to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination. Any authorized investigative agency may also request records maintained by any commercial

entity within the United States pertaining to travel by an employee in the executive branch of Government outside the United States.

(2) Requests may be made under this section where –

(A) the records sought pertain to a person who is or was an employee in the executive branch of Government required by the President in an Executive order or regulation, as a condition of access to classified information, to provide consent, during a background investigation and for such time as access to the information is maintained, and for a period of not more than three years thereafter, permitting access to financial records, other financial information, consumer reports, and travel records; and

(B)(i) there are reasonable grounds to believe, based on credible information, that the person is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(ii) information the employing agency deems credible indicates the person has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other information known to the agency; or

(iii) circumstances indicate the person had the capability and opportunity to disclose classified information which is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Each such request –

(A) shall be accompanied by a written certification signed by the department or agency head or deputy department or agency head concerned, or by a senior official designated for this purpose by the department or agency head concerned (whose rank shall be no lower than Assistant Secretary or Assistant Director), and shall certify that –

(i) the person concerned is or was an employee within the meaning of paragraph (2)(A);

(ii) the request is being made pursuant to an authorized inquiry or investigation and is authorized under this section; and

(iii) the records or information to be reviewed are records or information which the employee has previously agreed to make available to the authorized investigative agency for review;

(B) shall contain a copy of the agreement referred to in subparagraph (A)(iii);

(C) shall identify specifically or by category the records or information to be reviewed; and

(D) shall inform the recipient of the request of the prohibition described in subsection (b) of this section.

(b) *Prohibition of certain disclosure*

(1) *If an authorized investigative agency described in subsection (a) of this section 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 governmental or private entity, or officer, employee, or agent of such entity, may 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 such entity has received or satisfied a request made by an authorized investigative agency 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 persons 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 authorized investigative agency, any person making or intending to make a disclosure under this section shall identify to the requesting official of the authorized investigative agency 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 requesting official 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) of this section.

* * *

Author Contact Information

Charles Doyle
Senior Specialist in American Public Law
cdoyle@crs.loc.gov, 7-6968