Enforcing the Enforcer: Enhancing the FBI’s Accountability for the Use of National Security Letters

Joshua C. McDaniel

Available at: https://works.bepress.com/joshua_mcdaniel/1/
ENFORCING THE ENFORCER: ENHANCING THE FBI’S ACCOUNTABILITY FOR THE USE OF NATIONAL SECURITY LETTERS

Joshua C. McDaniel

In 2007, the U.S. Justice Department’s Office of the Inspector General issued the first in a series of three reports revealing that on thousands of occasions the FBI had improperly or illegally used its authority to issue national security letters. The national security letter enables the FBI to obtain confidential customer information from banks, ISPs, telephone companies, and other institutions without first obtaining a warrant or a grand jury subpoena and without the customer ever realizing.

This Comment argues that the abuses of NSL authority revealed in the Inspector General’s reports result significantly from the FBI’s lack of horizontal accountability (to the legislative and judicial branches and to other agencies within the executive branch) and vertical accountability (to individuals bringing lawsuits against the government or government officials). The absence of accountability is a unique feature of the FBI’s NSL authority and derives from the FBI’s need for secrecy in carrying out national security investigations.

Given the Inspector General’s findings of widespread abuse of the NSL authority, the case for reform is compelling. I offer two proposals that policymakers might consider. First, I propose the explicit creation of a statutory cause of action to affected individuals, along with a delayed disclosure mechanism intended to allow aggrieved individuals to learn of the FBI’s request of the individuals’ records. Second, I propose establishing an exclusionary rule for NSL-derived information, which would require certification in applications for FISA orders and in criminal proceedings of the validity of NSL-derived information. I argue that each of these proposals, though not comprehensive solutions, would enhance accountability and better protect individuals’ civil liberties while minimizing the costs in terms of the FBI’s ability to effectively carry out national security investigations.

INTRODUCTION .......................................................... 2
I. THE USE AND MISUSE OF NATIONAL SECURITY LETTERS ........................................ 6
   A. What is a National Security Letter? ........................................ 6
   B. Statutory Authorization for NSLS ................................... 7
   C. Origins and Growth of NSL Authority ................................. 8
      1. Origins of NSL Authority ............................................. 8
      2. The Patriot Act and the Subsequent Explosion in NSL Use .... 10
      3. NSLs in the Information Age: Nonstatutory Expansion of the FBI’s
         NSL Power ................................................................. 12
      4. The Patriot Reauthorization Act ..................................... 14
   D. Abuses of NSL Authority Revealed in the OIG Reports .......... 15
II. THE SOURCE OF NSL-ABUSE: LACK OF ACCOUNTABILITY .................. 18
    A. The FBI’s Institutional Predisposition ............................ 19
INTRODUCTION

In 2007, the U.S. Justice Department’s Office of the Inspector General (OIG) issued the first in a series of three reports revealing that on thousands of occasions the FBI had improperly or illegally used its authority to issue national security letters.\(^1\) The national security letter (NSL) is a demand letter that the FBI can send to certain kinds of private companies—such as banks, credit-reporting agencies, Internet service providers, and telephone companies—in order to secretly obtain private customer information. The NSL is a bread-and-butter tool that frequently serves as a gateway mechanism to more intrusive investigatory tools.

The statutes authorizing the FBI’s NSL authority allow the FBI to issue NSLs without first obtaining a warrant or a grand jury subpoena so long as the FBI certifies in the NSL that the customer’s records are “relevant to a national security investigation.”\(^2\) NSLs are unique among the various intelligence-gathering mechanisms at the disposal of the various federal agencies in that they

---


may be used to acquire information about U.S. citizens and residents who are not suspects in a national security investigation.\(^3\)

The OIG’s reports revealed that the FBI issued nearly 200,000 NSL requests from 2003 to 2006\(^4\) and that on thousands of occasions the FBI had circumvented federal privacy statutes and improperly obtained private information.\(^5\) Among the abuses uncovered by the OIG, the OIG highlighted that the FBI had requested and retained more information than it was authorized to obtain\(^6\) and had improperly used so-called “exigent letters.”\(^7\)

---

\(^3\) In fact, a majority (and increasing number) of NSLs target U.S. citizens and residents. See OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 at 111 (2008), available at http://www.justice.gov/oig/special/s0803b/final.pdf [hereinafter OIG 2008 REPORT] (“[T]he number of NSL requests generated from investigations of U.S. persons almost doubled from 6,159 in 2003 to 11,517 in 2006, which represented 57 percent of all NSL requests in that year.”). As discussed below, the predication standard for NSLs does not require individualized suspicion, but merely requires relevance to a national security investigation. See OIG 2007 REPORT at 8 (noting that the Patriot Act “eliminate[ed] the requirement that the information sought in an NSL must pertain to a foreign power or an agent of a foreign power and substitut[ed] the lower threshold that the information requested be relevant to or sought for an investigation to protect against international terrorist or espionage”).

\(^4\) See OIG 2008 REPORT at 9 (reporting that the FBI issued 192,499 NSL requests during the four-year period). According to the FBI’s periodic reports to Congress, the number of NSL requests in 2007, 2008, and 2009 concerning U.S. persons was 16,804, 24,744, and 14,788 respectively. Foreign Intelligence Surveillance Act Court Orders 1979–2009, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/wiretap/stats/fisa_stats.html (last visited March 24, 2011) [hereinafter FISA Court Statistics]. As a reference point, NSLs targeting U.S. persons climbed to 57 percent of all NSL requests in 2006, the last year reviewed by the OIG. OIG 2008 REPORT at 9.

\(^5\) See generally OIG 2007 REPORT at 66–107. For example, the OIG reported that in a sample of seventy-seven files, 22 percent “contained one or more possible violations relating to national security letters that were not identified by the FBI.” Id. at 122 (noting also that “[t]hese violations included infractions . . . , but also included instances in which the FBI issued national security letters for different information than what had been approved by the field supervisor). See also id. at 123 (noting that in the FBI’s Headquarters Counterterrorism Division over three hundred NSLs were improperly generated, with the result that “FBI agents did not generate and supervisors did not approve documentation demonstrating that the factual predicate required by the Electronic Communications Privacy Act, the Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, and internal FBI policy had been established”); id. (reporting that in an examination of four field offices “60 percent of the investigative files we examined contained one or more violations of FBI internal control policies relating to national security letters”).

\(^6\) See id. at 66–67 (summarizing basic categories of improper or illegal uses of NSL authority, including, among other categories relating to the receipt of too much information “obtaining . . . information concerning the wrong individuals” and “[o]btaining information that was not requested in the national security letter”).

\(^7\) See id. at 123 (describing the improper issuance of more than seven hundred exigent letters without first issuing NSLs). Although exigent letters are (at least arguably) a lawful means of
The OIG’s reports raise a difficult question: Given the FBI’s predisposition to prioritize national security above individual privacy interests and the FBI’s ability to operate without having to obtain a warrant or notifying the NSL targets, what is to keep the FBI’s use of NSLs in check? This Comment proposes two mechanisms designed to supplement ongoing efforts to increase the FBI’s accountability for its use of NSLs. First, this Comment proposes to make explicitly available a private cause of action to individuals whose information has been improperly accessed by the FBI, along with a delayed disclosure mechanism so that such individuals will be able to know about the potential violations. Second, this Comment proposes an exclusionary rule that would suppress evidence obtained in violation of the NSL-authorizing statutes when the government seeks to introduce such evidence in the Foreign Intelligence Surveillance Court (FISA Court) or in criminal court proceedings.

This Comment begins in Part I by describing what an NSL is and how the NSL is being used under the current statutory framework. I then discuss the ways in which NSLs create a significant privacy concern. Finally, I provide an overview of the abuses of NSL authority that have been reported in the 2007, 2008, and 2010 OIG Reports. As the OIG concludes, this Comment notes that while the FBI has unequivocally demonstrated its desire to comply with the recommendations set forth in the OIG reports and has already appeared to make visible improvements, achieving full compliance with existing NSL statutes requires continued monitoring and reinforcement by any effective means.

In Part II, I argue that the FBI’s noncompliance with laws and policies governing the use of NSLs results significantly from the FBI’s lack of accountability with respect to its use of NSLs. The FBI is institutionally predisposed to prioritize national security above civil liberties. I argue that, in

---

8 See OIG 2008 REPORT at A-5 (containing letter from FBI Director Muehlller).
9 See id. at 15 (“However, there are additional steps that the FBI is still considering and needs to take, and we believe that ensuring full compliance will require the continual attention, vigilance, and reinforcement by the FBI and the Department.”).
10 See Jon D. Michaels, All the President’s Spies: Private-Public Intelligence Partnerships in the War on Terror, 96 CAL. L. REV. 901, 922 (2008) (“Singularly tasked with protecting American lives and interests, the Executive is institutionally committed to facilitating the activities of its national-security and intelligence agencies.”).
the context of issuing NSLs, the FBI lacks both the belt and the suspenders of vertical and horizontal accountability. The FBI is sheltered from vertical accountability because NSLs almost always contain permanent gag orders and because national security investigations are of a necessity cloaked in secrecy. The FBI’s use of NSLs is further subject only to limited after-the-fact horizontal accountability. The FBI certifies its own NSLs and does not need to obtain a warrant or a grand jury subpoena. The USA PATRIOT Reauthorization and Improvement Act of 2005 (Patriot Reauthorization Act)\(^\text{11}\) created a form of meaningful accountability for the first time by directing the OIG to review the use and effectiveness of the FBI’s NSL authority from 2003 to 2006. This oversight reported and made publicly available its findings on the use (including the abuse) and effectiveness of the FBI’s NSL authority.

The audits performed by the OIG in addition to various bills proposed since the Patriot Reauthorization Act have done and likely will do much to curtail the amount of abuses of NSL authority. I conclude, however, that the question of how to keep in check the FBI’s use of its NSL authority while still permitting the FBI to carry out its essential investigative duties deserves continued attention.

Parts III and IV consider the two proposals set forth above: explicitly providing a statutory private cause of action to affected individuals, along with a delayed disclosure mechanism intended to allow aggrieved individuals to learn of the FBI’s request of the individuals’ records, and establishing an exclusionary rule for NSL-derived information, which would require certification in applications for FISA orders and in criminal proceedings of the validity of NSL-derived information. I argue that each of these proposals, though not comprehensive solutions, would enhance accountability and would encourage NSL-issuers to give pause to consider whether an NSL is proper.

With respect to the first proposal, I sketch the basic contours of the proposed cause of action. Furthermore, I address the question of how to deal with the need for secrecy by proposing a system of delayed declassification of such information as is necessary to sustain the cause of action, along with a procedure for maintaining still-sensitive information classified. For the second proposal, this Comment addresses the difficulties inherent in implementing additional procedural requirements in the FISA court and the costs of tagging NSL-derived information as coming from a particular NSL request. With each proposal, I conclude that, in spite of the costs, each proposal is a potentially cost-beneficial means of structurally encouraging accountability and greater concern for civil liberties while not overly restricting the FBI’s use of NSLs as an effective and necessary information discovery mechanism.

\(^{11}\) USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 119
I. THE USE AND MISUSE OF NATIONAL SECURITY LETTERS

National security letters (NSLs) are a relatively modern invention. Until recently, little was known publicly about the extent and character of the FBI’s use of NSLs. In recent years, however, increased scrutiny of the FBI’s use of NSLs by the media and by other government agencies has revealed a recent surge in the use of NSLs as well as widespread abuse of the NSL authority.

This Part first offers a snapshot of the FBI’s recent use of NSLs, including a brief discussion of the various NSL-authorizing statues. I then describe the origins and growth of NSL authority, highlighting the ways in which the FBI’s growing NSL authority has created increased oversight and transparency difficulties, as well as a much greater concern for privacy infringements. I then discuss the commission given to the OIG in the Patriot Reauthorization Act and the findings of widespread abuse of NSL authority—including the problems of underreporting, unaccountability, and unlawful behavior—in the OIG’s reports.

A. What is a National Security Letter?

In the four-year period from 2003 to 2006, the FBI issued a total of 192,499 national security letter requests.\textsuperscript{12} A national security letter (NSL) is a demand letter issued by the FBI\textsuperscript{13} to a private entity requiring the production of personal information about the entity’s customers.\textsuperscript{14} Similar to an administrative subpoena,\textsuperscript{15} NSLs are a form of compulsory process that the FBI may use to request private information. Using NSLs, the FBI can obtain customer

\textsuperscript{12} OIG 2008 REPORT at 9.
\textsuperscript{13} Although the FBI primarily has authority to issue NSLs, various authorities suggest that other agencies of the federal government may also possess NSL authority. See CHARLES DOYLE, CONG. RESEARCH SERV., NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE OF THE LEGAL BACKGROUND AND RECENT AMENDMENTS at i (2009) (noting that multiple government agencies responsible for foreign intelligence investigations, but principally the FBI, have authority to issue NSLs).
\textsuperscript{14} For an example copy of a national security letter, see http://www.eff.org/files/filenode/ia_v_mukasey/Nov2007_NSL.pdf.
\textsuperscript{15} “Administrative subpoena authority, including closely related national security letter authority, is the power vested in various administrative agencies to compel testimony or the production of documents or both in aid of the agencies’ performance of their duties.” Charles Doyle, Congressional Research Service, Administrative Subpoenas and National Security Letters in Criminal and Foreign Intelligence Investigations: Background and Proposed Adjustments at 1 available at http://www.fas.org/sgp/crs/natsec/RL32880.pdf; see also Erwin Chemerinsky, Essay: Civil Liberties and the War on Terror: Seven Years After 9/11 History Repeating: Due Process, Torture and Privacy During the War on Terror, 62 SMU L. REV. 3, 13 (2009) (describing national security letters as “a type of administrative subpoena that allows the government to obtain information about an individual, even highly personal information, simply by sending a demand letter”).
information from telecommunications providers, financial institutions, credit agencies, travel agencies, and other institutions. In most cases, the FBI then compiles NSL-derived information, much of which is made available to other government agencies.\textsuperscript{16}

NSLs are considered to be one of the bread-and-butter tools in the FBI’s arsenal of information gathering techniques.\textsuperscript{17} By discovering the websites that a person visits, the email addresses with which a person has corresponded, the financial transactions that a person has engaged in, and more, the FBI obtains information that enables it to obtain further authorizations.\textsuperscript{18} NSLs are unique in that they allow the FBI to obtain such private information from third parties without obtaining a warrant or a grand jury subpoena so long as the issuer complies with statutory certification requirements.\textsuperscript{19} Moreover, the OIG’s 2006 audit revealed that 97 percent of a random sample of NSLs contained a gag order, requiring that the recipient generally not tell anyone about the NSL demand.\textsuperscript{20}

B. Statutory Authorization for NSLs

The FBI is able to issue five types of NSLs, each known by the relevant federal act, authorizing its use. Each type of NSL allows the FBI to obtain different kinds of information from different entities. The five types of NSLs are the following:\textsuperscript{21}

\begin{itemize}
  \item \textsuperscript{16} See OIG 2008 REPORT at 73–74 (“[M]uch of the information in FBI databases [including in particular information from electronic communication records derived from ECPA NSLS] is periodically transferred to the Investigative Data Warehouse. According to the FBI, the Investigative Data Warehouse contains data from 53 different sources and is available to over 13,000 Special Agents, analysts, and law enforcement partners around the world.”).
  \item \textsuperscript{17} See OIG 2007 REPORT at xxii (“Many FBI personnel used terms to describe NSLs such as ‘indispensable’ or ‘our bread and butter.’”); Orin Kerr, More on National Security Letters, VOLOKH CONSPIRACY, Nov. 15, 2005 12:54 PM, http://volokh.com/posts/1132080893.shtml (quoting Michael J. Woods) (“In the counterintelligence/counter-terrorism business, NSLs are unglamorous, journeyman tools that historically garnered far less attention than the more intrusive search and surveillance authorities found in the Foreign Intelligence Surveillance Act (FISA).”)
  \item \textsuperscript{18} See OIG 2007 REPORT at xxii (listing as one of the principal uses for NSLs the establishment of “evidence to support FISA applications to the FISC for electronic surveillance, physical searches, or pen register/trap and trace orders”).
  \item \textsuperscript{19} For example, the ECPA-NSL may only be issued upon certification that 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 on the basis of activities protected by the first amendment to the Constitution of the United States.” 18 U.S.C. § 2709(b)(2) (2006). The certification requirement found in each of the NSL statutes is a variation on this theme.
  \item \textsuperscript{20} OIG 2008 REPORT at 10.
  \item \textsuperscript{21} For a more in-depth profile of each of the current NSL statutes, see Table 1 of DOYLE CRS REPORT at http://www.fas.org/sgp/crs/intel/RS22406.pdf.
\end{itemize}
• ECPA NSL: A customer’s name, address, length of service, and toll billing info (includes telephone numbers and email addresses, but not the content of such communications) may be demanded of a telecommunications provider.\(^{22}\)

• RFPA NSL: Information concerning open and closed checking and savings accounts, records, and other transactions may be requested from a variety of financial institutions.\(^{23}\)

• FCRAu NSL: Information about an individual’s credit history—including the names and addresses of all financial institutions at which a consumer maintains or has maintained an account and identifying information limited to name, current address, former addresses, and places of employment—may be obtained from consumer credit agencies.\(^{24}\)

• FCRAv NSL: Full credit reports may be obtained from consumer credit agencies.\(^{25}\)

• NSA NSL: Information may be obtained from financial institutions, consumer credit agencies, and travel agencies in connection with investigations of improper disclosure of classified information by government employees.\(^{26}\)

Historically, the vast majority of NSLs have been of the ECPA variety.\(^{27}\)

Because such a large percentage of NSLs are ECPA-NSLs, this Comment focuses primarily on the use, problems, and solutions regarding the NSL authorization and other provisions of the ECPA.

C. Origins and Growth of NSL Authority

1. Origins of NSL Authority

In 1978, the passage of the Right to Financial Privacy Act (RFPA) marked the appearance of the original predecessor to the modern-day NSL. The RFPA was intended to provide broad safeguards for individual privacy.\(^{28}\) The forerunner of the NSL was contained in an exception to the RFPA’s prohibition to financial entities against disclosing customer information. The exception

\(^{27}\) Id. at xviii (“The overwhelming majority of the NSL requests sought telephone toll billing records information, subscriber information (telephone or e-mail), or electronic communication transactional records under the ECPA NSL statute.”).
\(^{28}\) The RFPA was a response to the Supreme Court’s decision in United States v. Miller. See Andrew E. Nieland, Note, National Security Letters and the Amended Patriot Act, 92 CORNELL L. REV. 1201, 1208 (2007).
provided that such entities could disclose certain types of private information to
the FBI if the FBI certified that a national security threat existed. Notably, this
national security exception was voluntary, not compulsory.29

In the years following the creation of the national security exception of the
RFPA, the FBI began to issue letters to telecommunications providers requesting
telephone records. These requests eventually came to be known by the FBI as
“national security letters.”30 Just as with the RFPA exception, however, the FBI
had no compulsory power to demand desired information.

The year 1986 marked the statutory creation of the first compulsory NSLs. 
Congress provided NSL authority to the FBI in a 1986 amendment to the RFPA
and in the newly enacted Electronic Communications Privacy Act (ECPA).31 The
two initial types of NSL authority, which were eventually supplemented by the
FCRAu and FCRAv NSLs in 1995(?), largely went unnoticed. “In the mid-1990s,
Congress added two more NSL provisions—one permits NSL use in connection
with the investigation of government employee leaks of classified information
under the National Security Act, the other grants the FBI access to credit agency
records pursuant to the Fair Credit Reporting Act, under much the same
conditions as apply to the records of financial institutions.”32

29 See id. at 1206 (“NSLs began as an alternative to compulsory process—a way to ‘override’
privacy legislation. . . .”); see also CHARLES DOYLE, CONGRESSIONAL RESEARCH SERVICE,
NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE OF THE
LEGAL BACKGROUND AND RECENT AMENDMENTS at i (2009) (“[The RFPA] removed the
restrictions on the release of customer information imposed on financial institutions by the RFPA,
but it then left them free to decline to comply when asked to do so.”).
30 See Nieland, supra note 28, at 1208 (“Oddly enough, by 1986, the FBI was referring to such
requests as ‘national security letters.’” See also S. Rep. No. 99-307, at 15 (1986); see also OIG
2007 Report at 7 n. 8 (noting that the term “national security letter” did not originally appear in
any of the NSL-authorizing statutes and that the “term was first used in legislation in the Patriot
Reauthorization Act”).
31 See CHARLES DOYLE, CONGRESSIONAL RESEARCH SERVICE, NATIONAL SECURITY LETTERS IN
FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE OF THE LEGAL BACKGROUND AND RECENT
AMENDMENTS at i (2009); see also Nieland, supra note 28, at 1209 (“The FBI sought
congressional intercession [in response to resistance], which Congress granted to a limited extent
in section 201 of the Electronic Communications Privacy Act of 1986 (ECPA).”).
32 CHARLES DOYLE, CONGRESSIONAL RESEARCH SERVICE, NATIONAL SECURITY LETTERS IN
FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE OF THE LEGAL BACKGROUND AND RECENT
AMENDMENTS at i (2009).
2. The Patriot Act and the Subsequent Explosion in NSL Use

The USA PATRIOT Act (Patriot Act),33 adopted on October 26, 2001, greatly expanded the federal government’s law enforcement powers.34 Although largely overlooked at the time, the Patriot Act’s changes to NSL authority were significant and highly influential.35

The Patriot Act brought about two key changes to the FBI’s NSL authority. Perhaps the most significant change to NSL authority was the elimination of the requirement that the subject of the investigation sought be a foreign power or an agent of a foreign power.36 Prior to the Patriot Act, the predication standard for NSLs required that the FBI provide “specific and articulable facts giving reasons to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power.”37 Under the Patriot Act, NSLs can request information regarding any individual within the United States—even a U.S. citizen—so long as the information sought is “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities . . . .”38 By 2005, the OIG estimated that more than 50 percent of all NSLs issued were NSLs generated from investigation of U.S. persons.39 This much lesser standard resulted in many NSLs targeting U.S. citizens and residents with no obvious connections to terrorism.40

34 See Erwin Chemerinsky, Civil Liberties and the War on Terrorism, 45 WASHBURN L.J. 1, 14 (“[The Patriot Act] is 342 pages long and is difficult to read because it is filled with references to other provisions of the United States Code.”). “The very expansive definition of terrorism in the Patriot Act . . . give[s] rise to its broad application by law enforcement, including in cases that are not related to terrorism.” Id. See also id. at 15 (describing the Patriot Act’s definition of “domestic terrorism” as “incredibly sweeping”).
36 Section 505 of the Patriot Act; see also Barton Gellman, The FBI’s Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans, WASH. POST, Nov. 6 2005 (“The Patriot Act, and Bush administration guidelines for its use, transformed those letters by permitting clandestine scrutiny of U.S. residents and visitors who are not alleged to be terrorists or spies.”).
38 Pub. L. 107-56 § 505. Section 505 similarly expanded the FBI’s RFPA-NSL and FCRAu-NSL authorities. Id.
39 See OIG 2007 REPORT at xx (“The percentage of NSL requests generated from investigations of U.S. persons increased from about 39 percent of all NSL requests in CY 2003 to about 53 percent of all NSL requests in CY 2005.”).
40 See Eric Lichtblau, F.B.I. Data Mining Reached Beyond Initial Targets, N.Y. TIMES, Sept. 9, 2007 (describing targeting of “community of interest” of targets—“the network of people that the target was in contact with”); Barton Gellman, The FBI’s Secret Scrutiny: In Hunt for Terrorists,
The Patriot Act further provided greater administrative flexibility to the process by widening the circle of FBI leaders capable of signing NSLs from FBI headquarters officials to include Special Agents in Charge in FBI field offices. 41

Soon after the passage of the Patriot Act, there was a sea change in NSL usage. The FBI went from issuing hundreds of NSLs per year to issuing tens of thousands of NSLs per year. 42 In 2009, the FBI issued 14,788 NSLs generated from investigations of U.S. persons alone. 43 Thus, “the amendments [a]ve the FBI . . . something that it had been unable that it had been unable to obtain through more overt political channels – a remarkably robust administrative subpoena power.” 44 While the changes brought about by the Patriot Act clearly brought benefits in terms of efficiency, 45 the substantial increase in NSL use in

41 Pub. L. 107-56 § 505. The Patriot Act also provided the FBI with an additional NSL authority to obtain consumer full credit reports in international terrorism investigations pursuant to an amendment to the Fair Credit Reporting Act (FCRA). 15 U.S.C. §1681(v) (Supp. IV 2005).

42 The DOJ’s Inspector General has estimated that the tally of NSLs issued per year has jumped from 7800 in 1999 and 8500 in 2000 to 39,346 NSL requests in 2003; 56,507 in 2004; 47,221 in 2005; and 49,425 in 2006. OIG 2007 REPORT at xix, 44 n. 84, http://www.usdoj.gov.oig/special/s0703b/final.pdf; OIG 2008 REPORT at 9. “These numbers, though high, substantially understate the number of NSL requests actually issued, because the FBI has not kept accurate records of its use of NSLs. The OIG sampled 77 FBI case files and found 22 percent more NSL requests in the case files than were recorded in the FBI’s NSL database.” Testimony of Jameel Jaffer, at 5, available at http://judiciary.house.gov/hearings/pdf/Jaffer080415.pdf (citing OIG 2007 REPORT at 32). It is estimated that usage of NSLS was in the “hundreds” during the earlier years of usage. See Nieland, supra note 28, at 1202–03 n.9 (citing Ashcroft saying that the estimate is on the “long time span” between the passage of the first NSL statute and the present day, etc).


44 Nieland, supra note 28, at 1206. Another change that occurred following the passage of the Patriot Act occurred when the Attorney General issued the NSI Guidelines in 2003 permitting NSLs to be used during preliminary investigations (rather than only during full investigations. OIG 2007 REPORT at 40. Over 40 percent of a sample of 293 NSLs were examined during preliminary investigations. Id.

45 See id. at 43 (noting that FBI personnel stated that the infrequent use of NSLS prior to the passage of the Patriot Act was attributable in part to the “lengthy process required to obtain national security letters,” which made it so that “NSLS generally were not viewed as an effective investigative tool”).
the years following also increased the potential that American individuals’ privacy interests would be infringed in the course of national security investigations.\textsuperscript{46} 

### 3. NSLs in the Information Age: Nonstatutory Expansion of the FBI’s NSL Power

In addition to the NSL’s statutory expansions, technological and cultural changes in recent years have expanded the FBI’s NSL authority in two ways.\textsuperscript{47} First, similar to Moore’s law, the amount of information communicated or stored electronically seems to be increasing exponentially. With all of the advantages that flow from electronic communications, consumers also entrust ever-increasing amounts of data in the hands of entities such as telecommunications providers.\textsuperscript{48} As the amount of private information placed in the hands of such entities increases, there is a corresponding increase in the amount of information attainable by NSLs. Although the FBI may not use NSLs to request the substance of electronic communications—for example, the subject heading, main text, and attachments of emails—the FBI may nevertheless discover a significant amount of information with just a ECPA NSL:

\[\text{[A]}\text{n Internet service provider can be compelled to disclose a subscriber’s name, address, telephone number, account name, e-mail address, and credit card and billing information. It can be compelled to disclose the identities of individuals}\]

\textsuperscript{46}See Michaels, supra note 10, at 949 (“While there is good reason to keep the ex ante requirements to a minimum (e.g., to permit rapid responsiveness in emergency situations), inevitably there is a cost associated with giving intelligence agents wider discretion to commence operations, and thus there ought to be a correspondingly greater need for corrective tools to remedy instances (not to mention patterns) of overreaching or abuse.”).

\textsuperscript{47}“[T]he breadth of NSL authority expanded not merely overtly through legislative amendment, but also covertly through technological change.” Nieland, supra note 28, at 1206.

\textsuperscript{48}See DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1 (2004) (“It is ever more possible to create an electronic collage that covers much of a person’s life—a life captured in records, a digital person composed in the collective computer networks of the world.”); id. at 167–68 (describing the enormous information-gathering capabilities of the Internet); Miguel Helft & Claire Cain Miller, 1986 Privacy Law Is Outrun by the Web, N.Y. TIMES, A1 (Jan. 10, 2011), available at http://www.nytimes.com/2011/01/10/technology/10privacy.html?_r=1&hp (“As Internet services—allowing people to store e-mails, photographs, spreadsheets and an untold number of private documents—have surged in popularity, they have become tempting targets for law enforcement.”); see generally Deirdre K. Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 GEO. WASH. L. REV. 1557 (2004) (arguing that the “changed ways in which people use the Internet” has “exposed fundamental weaknesses in the structure of the ECPA” and that “[i]t is time to revisit and revise ECPA to establish appropriate privacy protections that respect individuals’ expectations and constitutional requirements”)
who have visited a particular website, a list of websites visited by a particular individual, a list of e-mail addresses with which a particular individual has corresponded, or the e-mail address and identity of a person who has posted anonymous speech on a political website.\footnote{49} Although any given piece of information may not be particularly revealing, when such information is compiled, cross-referenced, and analyzed, the whole is greater than the sum of its parts.\footnote{50}

Perhaps more importantly, the FBI may use NSL-derived information—even if obtained improperly—to support FISA applications for more invasive information-gathering techniques.\footnote{51} The FBI may piece together each item of information like puzzle pieces until the puzzle is assembled and the larger picture is revealed.

A second way that advancements in technology have led to increased privacy concerns is the evolution in the FBI’s ability to analyze the data received. Since the passage of the Patriot Act, the FBI’s techniques for analyzing and drawing conclusions from already gathered information have increased.\footnote{52} This is


\footnotetext{50}{See OIG 2007 REPORT at xxiv (“Analysis of subscriber information for telephone numbers and e-mail addresses also can assist in the identification of the investigative subject’s family members, associates living arrangements, and contacts. If the subject’s associates are identified, case agents can generate leads for their squad or another FBI field division, the results of which may complement the information obtained from the original NSL.”). Information obtained by a RFPA-NSL can similarly reveal a significant amount about the target. See id. (“Analysis of [RFPA-NSL-derived] data also can reveal the identity of the financial institutions used by the subject; the financial position of the subject; the existence of overseas wire transfers by or to the subject . . . ; loan transactions; evidence of money laundering; the subject’s involvement in unconventional monetary transactions, including accounts that have more money in them than can be explained by ordinary income or the subject’s employment; the subject’s financial network; and payments to and from specific individuals.”).}

\footnotetext{51}{See id. (“The FBI also informed us that the most important use of ECPA national security letters is to support FISA applications for electronic surveillance, physical searches, or pen register/tap and trace orders.”). Further financial information regarding an individual, such as “consumer full credit reports, including records of individual accounts, credit card transactions, and bank account activity,” may be obtained through NSLS issued pursuant to the FCRA. Id. at xxiv–xxv.}

\footnotetext{52}{See id. at 44 (“[T]he FBI’s increased analytical capabilities in recent years has changed the perspective of FBI personnel on the use and effectiveness of national security letters.”). Some advancements in governmental analytical capabilities have been questioned, such as the Department of Defense’s program originally called “Total Information Awareness.” See DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 5 (2004) (describing the Department of Defense’s development in 2002 of the Total Information Awareness program, which involved the collection of person information from private-sector sources and the}
particularly significant given that much of the data obtained from tools like NSLs is often pooled together and retained indefinitely.\(^{53}\)

The combination of such expansions of the FBI’s NSL authority means that the FBI’s NSL authority is becoming increasingly at odds with the original NSL power held by the FBI in the 1980s and 1990s\(^ {54}\) and with individuals’ expectations of privacy.\(^ {55}\) Furthermore, the significant and growing potential for infringement to individuals’ civil liberties that NSLs cause creates greater concern for establishing adequate safeguards to protect data that is potentially retrievable by NSLs.

4. The Patriot Reauthorization Act

The Patriot Reauthorization Act, and some of the court cases it followed, brought much-needed attention and accountability tools to the FBI’s use of NSLs. Despite the significant increase in NSL issuance in the years following the passage of the Patriot Act, NSLs received little public attention until 2004.\(^ {56}\) (The lack of public attention may have been attributable to the fact that no one really

\[^{53}\text{See OIG 2008 REPORT at 70–72 ("[I]nformation related to individuals determined not to be of interest or concern to law enforcement also would be retained on the chance that the information could become relevant in the future.").}]

\[^{54}\text{Orin Kerr, More on National Security Letters, VOLOKH CONSPIRACY, Nov. 15, 2005 12:54 PM, http://volokh.com/posts/1132080893.shtml (quoting Michael J. Woods) ("NSLs reflect tensions between evolving technology and the increasing inadequate consent-based theory behind Miller. NSLs developed in a limited context: the users of NSLs (FBI counterintelligence agents) had discretionary access to the authorities, but were regulated by fairly strict guidelines and by the legal standard (‘specific and articulable facts’) embedded in the NSL statutes. At the same time, the utility of the ‘transactional information’ available from an NSL was limited by the trivial nature of the information itself and the FBI’s lack of technical or legal ability to do much with it. The PATRIOT Act and subsequent revisions of the FBI’s operating guidelines significantly lowered the legal standards, devolved NSL issuing authority to FBI field offices, and even extended one species of NSL to an indeterminate list of other government agencies. The general impetus toward information-sharing among government entities and the massive investment in technical solutions may eventually deliver to the government the ability to process data efficiently. Finally, the rate at which individuals shed transactional data simply by living in a networked world seems to increase daily. The composite picture of individual activity that can emerge from such data is often of startling clarity, and will likely sharpen with in the future.").}]

\[^{55}\text{See DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 167 (2004) (describing the “false sense of privacy” that individuals have while using the Internet).}]

\[^{56}\text{Nieand, supra note 28, at 1203.}\]
knew how many NSLs were being issued.) In 2004, however, NSLs went from relative obscurity to the forefront of national debate when the plaintiff ISP in *Doe v. Gonzales* challenged the gag order in order to be able to publicly reveal that they had received an NSL.\(^{57}\) The court eventually held that the gag order placed upon NSL recipients violated the recipient’s First Amendment right of free speech.\(^{58}\) In the process, NSLs began to receive widespread media attention.\(^{59}\)

Given that the vast majority of NSLs contain (and depend upon) the gag order provision, action by Congress to cure the constitutional defect seemed necessary. Congress indeed made key changes to the NSL provisions, especially as relating to the gag order provisions of the NSL-authorizing statutes, with the passage of the USA PATRIOT Improvement and Reauthorization Act of 2005 (Patriot Reauthorization Act).\(^{60}\) Among other changes,\(^{61}\) a key provision of the Patriot Reauthorization Act was the call for audits by the Justice Department’s Office of the Inspector General. As I discuss further in Part II of this Comment, these changes constituted an important first step in establishing an effective accountability regime for the FBI’s use of NSLs.

**D. Abuses of NSL Authority Revealed in the OIG Reports**

A key part of the Reauthorization Act was the direction to the Department of Justice Office of Inspector General to review the FBI’s use of NSLs for two time periods—CY 2003 and 2004 and then CY 2005 and 2006. The Reauthorization Act specified that the OIG was to examine both the use and effectiveness of national security letters.\(^{62}\) The OIG conducted the reviews and

---

\(^{57}\) See id. at 1205.

\(^{58}\) For a description of the case, see CHARLES DOYLE, CONGRESSIONAL RESEARCH SERVICE, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE OF THE LEGAL BACKGROUND AND RECENT AMENDMENTS 3–4 (2009).

\(^{59}\) See Nieland, supra note 28, at 1205 (“In November 2005, NSLs moved from the metro section to the front page when the Washington Post published a report claiming that the FBI had issued over 30,000 letters per year since the passage of the Patriot Act.”).


\(^{61}\) The Reauthorization Act provided for judicial enforcement of NSLs and provided for judicial review of both the requests and accompanying nondisclosure requirements. CHARLES DOYLE, CONGRESSIONAL RESEARCH SERVICE, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE OF THE LEGAL BACKGROUND AND RECENT AMENDMENTS 3 (2009). The Act further declared that gag order provisions should contain necessary exceptions (such as the ability to consult an attorney). It is important to note here that the new provisions of judicial review of the requests and accompanying nondisclosure requirements were effectively made available only to the recipient, not the target, of NSL requests. In most cases, it seems unlikely that an NSL recipient would have the necessary incentive to sue and vigorously litigate a claim that an NSL is invalid.

\(^{62}\) The Reauthorization Act directed the OIG to conduct:
made publicly available a series of three reports in the years 2007, 2008, and 2010. The OIG discovered a variety of problems, noting that the improper or illegal use of the FBI’s NSL authority could be divided into the following categories:

- Issuing national security letters when the investigative authority to conduct the underlying investigation had lapsed;
- Obtaining telephone toll billing records and e-mail subscriber information concerning the wrong individuals;
- Obtaining information that was not requested in the national security letter;
- Obtaining information beyond the time period referenced in the national security letter;
- Issuing [FCRA NSLs] seeking records that the FBI was not authorized to obtain through an NSL in the pending investigation under the referenced statute, such as issuing FCRA consumer full credit report national security letters in counterintelligence investigations;
- Issuing improper requests under the statute referenced in the NSL such as issuing an ECPA national security letter seeking an investigative subject’s

Patriot Reauthorization Act § 119(b).

63 The OIG elected to include CY 2005 in the first report. Thus, the 2007 report covered CY 2003 to 2005. The 2008 report covered CY 2006. The third report was prepared by the OIG’s own discretion in order to add additional detail to some of the violations that had been uncovered, particularly focusing on the FBI’s use of exigent letters.
educational records, including applications for admission, emergency contact information, and associations with campus organizations;

- Obtaining telephone toll billing records by issuing “exigent letters” signed by a Counterterrorism Division Unit Chief or subordinate personnel rather than by first issuing duly authorized national security letters pursuant to the ECPA NSL statute; and

- Issuing national security letters out of “control files” rather than from investigative files” in violation of FBI policy.\(^{64}\)

An additional problem with the FBI’s use of NSLs uncovered by the OIG was the systematic underreporting of data regarding NSLs to Congress. The OIG traced the problem to the underrecording of NSLs and NSL requests in the OGC (the FBI’s Office of General Counsel) database (maintained by the OGC). The numbers and data in this database are those used to report to Congress. The OIG estimated that approximately 6 percent of the NSL requests issued by the FBI during the period under review were missing from the OGC database.\(^{65}\)

Perhaps the most notable problem reported by the OIG was the use of “exigent letters” to obtain private information. The OIG reported that “on over 700 occasions the FBI obtained telephone toll billing records or subscriber information from 3 telephone companies without first issuing NSLs or grand jury subpoenas. Instead, the FBI issued so-called ‘exigent letters’ signed by FBI Headquarters Counterterrorism Division personnel who were not authorized to sign NSLs.”\(^{66}\)

The exigent letters stated that there were “exigent circumstances” and often promised future NSLs or grand jury subpoenas.\(^{67}\) The OIG further reported that, in general, NSLs and grand jury subpoenas did not follow. Moreover, in many cases, there were no exigent circumstances.\(^{68}\)

Part of the problem was that there was a significant amount of collusion between the telecommunications providers and the FBI in circumventing the NSL process. The OIG Report stated that these exigent letters arose in part due to statutory justification. What was particularly troublesome was that the extent of

\(^{64}\) OIG 2007 REPORT at 66–67.

\(^{65}\) Id. at xvii (“As a result of the delays in uploading NSL data and the flaws in the OGC database, the total numbers of NSL requests that were reported to Congress semiannually in CYs 2003, 2004, and 2005 were significantly understated . . . . [W]e estimated that approximately 8,850 NSL requests, or 6 percent of NSL requests issued by the FBI during this period were missing from the database.”).

\(^{66}\) Id. at xxxiv.

\(^{67}\) See id. at 97.

\(^{68}\) Id. (“[T]he FBI made factual misstatements in its official letters to the telephone companies either as to the existence of an emergency justifying shortcuts around lawful procedures or with respect to steps the FBI supposedly had taken to secure lawful process.”).
the collaboration between the telecommunications provider and the FBI. The OIG reported that “[i]n 2003 and 2004 the FBI entered into contracts with three communications service providers requiring the communications service providers to place their employees in the CAU’s office space and to give these employees access to their companies’ databases so they could immediately service FBI requests for telephone records.”69 Under one contract in particular, the company’s analysts performed functions as focusing attention on a “community of interest,” monitoring for priority indicators, and evaluating telephone data.70 In one office, a unit of the telecommunications provider had staff on site for the FBI. In fact, it was personnel of the telecommunications provider that raised the idea of exigent letters. The company would sift through information to detect anything that the FBI might have interest in. If such were the case, the FBI had access to a form exigent letter that it would prepare and then send to the FBI for the needed signature. In one reported instance, sticky notes were used to communicate information between the two offices.

What makes matters worse is that information improperly obtained by an exigent letter or the like is retained in the FBI’s databases and shared with other state and local law enforcement agencies.71

Additionally, the OIG reported on the use of so-called “blanket NSLs.” Blanket NSLs are defined as NSLs “issued . . . in connection with efforts to issue legal process to cover information already acquired through exigent letters and other informal requests.”72 In other words, blanket NSLs are NSLs that are intended to cover up prior improperly issued informal requests such as exigent letters in an attempt to meet statutory muster. Often one blanket NSL was used to apply to a large number of separate requests.73

In sum, the degree and diversity of improper and illegal uses of the FBI’s NSL authority uncovered in the OIG’s reports are clearly significant.

II. THE SOURCE OF NSL-ABUSE: LACK OF ACCOUNTABILITY

Given the significance of the privacy concerns at stake, the question of how to resolve the problems identified in the OIG Reports is particularly

69 OIG 2010 REPORT at 20. The OIG reported that two of the companies each assigned one full-time employee and the third company rotated four analysts through two full-time positions. Id. at 20 n. 23.
70 Id. at 22.
71 See Jeffrey Rosen, Who’s Watching the F.B.I.?, N.Y. TIMES, April 15, 2007 (“[E]ven if F.B.I. agents clear the subject of a national-security letter, they store the information gleaned from it in digital databases that include more than a half-billion records, are not purged for at least 20 years and can be shared with state law-enforcement agencies or with private businesses for data mining.”).
72 OIG 2007 REPORT at 127.
73 See id. at 127 for discussion of problems associated with blanket NSLs.
important. In this Part, I address the “why” of the problem: Why has the FBI—an agency that is concerned with investigating and enforcing violations of the law—violated privacy statutes on a widespread basis? I argue that the FBI’s improper or illegal uses of NSLs stem from a combination of the FBI’s institutional predisposition to prioritize national security with the FBI’s insufficient accountability for its use of its NSL authority.

It would seem that increased regulation is not a good answer to the question of how to stop the FBI’s improper use of NSLs. One particular finding of the OIG’s 2008 Report was that despite the finding that “significant limitations already exist[ed] governing the proper use of NSLs, . . . notwithstanding these controls, we found serious abuses of NSL authorities . . . .”74 Regulations relating only to the internal conduct of the FBI do not get at the root of the problem.

In this Part, I begin by describing the FBI’s institutional predisposition to aggressively protect national security. I conclude that, absent some counterbalance, the FBI, in its pursuit of maintaining national security, will fail to adequately account for the protection of civil liberties, such as the freedom from unexpected invasion of privacy. I then argue that the FBI is not accountable for its use of NSLs sufficient to counterbalance its institutional predisposition. Recognizing that the term “accountability” is ambivalent, I first discuss what I mean by it. In so doing, I observe that the FBI is not sufficiently accountable in multiple respects—principally with regard to vertical and horizontal accountability. I then discuss the promising steps that Congress has taken and has proposed to take to increase accountability. Although these actions and proposals are a good step in the right direction, I conclude that more steps should be taken, so long as the benefits of such steps are not outweighed by the potentially significant national-security costs.

A. The FBI’s Institutional Predisposition

The FBI is institutionally committed to immediately respond to national security threats. The FBI is a “threat-based and intelligence-driven national security organization.”75 Chief among the FBI’s priorities is the protection of the United States from terrorist attack and foreign intelligence operations and

---

74 OIG 2008 REPORT at 69.
75 Quick Facts, FEDERAL BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/quick-facts/quickfacts (last visited March 23, 2011). The FBI’s mission “is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.” Id.
This is not a bad thing—we do not want to overly constrict the FBI’s abilities. In fact, the FBI’s focus on law enforcement and national security reflects one of the core benefits of the doctrine of separation of powers: the specialization and efficiency gains derived from the division of labor. Given the at-times very high stakes involved with defending national security, the FBI is tasked with aggressively protecting the United States.

On the other hand, the danger is that the government agents tasked with protecting national security will unduly compromise individuals’ civil liberties in the process. Rather than dealing with the difficult question of how to identify the ideal balance between national security and civil liberties, my approach in this Comment is to assess whether certain changes to the status quo would result in a net improvement—that is, the increased protection of civil liberties would outweigh the costs in terms of national security.

The FBI’s institutional predisposition is key here. Other branches or agencies of the federal government are more inclined to consider the costs in terms of civil liberties. The legislative branch is institutionally prone to consider civil liberties in part because of the ideological diversity within Congress. The “separation of parties” inherent in Congress will ensure that there should always be a critical mass of members of Congress whose ideological preferences and constituencies demand a more robust protection of civil liberties. This is not to say that Congress will always rein in overreaching by the executive branch with regard to the balance between national security and civil liberties, especially when there is no “separation of parties” among the two chambers of Congress and the executive branch. It can at least be said with some confidence that Congress is more institutionally predisposed to consider civil liberties than the FBI.

Similarly, the judicial branch is more predisposed to consider civil liberties. Setting aside the ideological preferences or sympathies of judges or juries, parties often bring suit in order to vigorously seek redress for

---

76 Id. (listing the FBI’s priorities and noting that “in executing the following priorities, we will produce and use intelligence to protect the nation from threats and to bring to justice those who violate the law”).


78 See Note, Mechanisms of Secrecy, 121 HARV. L. REV. 1556, 1559–60 (2008) (“Optimal arrangements will not necessarily be ones that maximize public officials’ compliance with the public’s wishes, but will be those that produce the greatest net benefits: the value of public-regarding actions of government minus the cost of monitoring and bonding.”).


80 See Note, supra note 78, at 1559–60 (“Simply setting up one branch of government to monitor another will work only when there is reason to think that the monitor actually will police the other branch’s activities effectively.”).
infringements of civil liberties. Similar to the institution of debate and difference within Congress, the court system’s adversarial approach to resolving disputes ensures that civil liberties will at least be strongly considered. Finally, the OIG, although it is an agency of the executive branch, is more inclined to weigh the interest of civil liberties in carrying out its work. Whether because of a desire to competently carry out the direction of Congress or its general purpose to “inspect,” the OIG has been viewed as an effective monitor of the FBI’s conduct.

The FBI’s strong institutional predisposition to subordinate civil-liberty concerns to the defense of national security increases the likelihood that the FBI will circumvent the strictures of privacy statutes, perhaps to the point of making such actions inevitable. I now turn to addressing how enhanced accountability can serve to counterbalance the FBI’s institutional predisposition to prioritize the defense of national security.

B. The Belt and Suspenders of Accountability

Rather than expecting the FBI to independently keep its own actions in check, I argue here that enhancing the FBI’s accountability is a viable means of adequately maintaining the integrity of privacy protections that improper NSLs violate. The term “accountability” has various potential meanings. For purposes of this Comment, I have chosen to begin with the distinction between horizontal and vertical accountability. I take horizontal accountability to mean accountability between the FBI and other branches or agencies of the federal government. I use the term vertical accountability to mean accountability between the FBI and “the people.” In general, having both horizontal and vertical accountability is ideal, especially given that each form of accountability has certain limitations, as discussed below.

In the following Subparts, I discuss various ways in which (1) horizontal accountability and (2) vertical accountability are lacking. I place particular

81 See Andreas Schedler, Conceptualizing Accountability, in The Self-Restraining State: Power and Accountability in New Democracies 13, 13 (Andreas Schedler, Larry Diamond, & Marc F. Plattner eds., 1999) (“[A]ccountability represents an underexplored concept whose meaning remains evasive, whose boundaries are fuzzy, and whose internal structure is confusing.”). Schedler asserts that “political accountability carries two basic connotations: answerability, the obligation of public officials to inform about and to explain what they are doing; and enforcement, the capacity of accounting agencies to impose sanctions on powerholders who have violated their public duties.” Id. at 14.

82 This includes agencies of the executive branch, such as the Department of Justice’s Office of the Inspector General, that are “further removed from the immediate pressures of combating terrorism.” Michaels, supra note 10, at 950.

83 Although vertical accountability primarily refers to the accountability that government actors face by means of the electoral process, my view is broader and includes accountability of governmental actors and organizations through the adjudicatory system.
emphasis on assessing whether transparency, justification, and enforcement are required or permitted under the current NSL regime.  

1. Horizontal Accountability

Horizontal accountability is accountability of a governmental actor or organization to another segment of the government. Various distinctions can be made within horizontal accountability, such as intra-executive branch (meaning for most agencies accountability of the agency to the Department of Justice), intra-agency (such as accountability between the DOJ’s FBI and the DOJ’s OIG), and inter-branch accountability (such as accountability between Congress or the courts and the executive branch). Clearly accountability can exist even within the FBI (for example, if a specific unit within the FBI is tasked with discovering violations and personnel causing such violations are subject to disciplinary measures imposed by the FBI).

Although intuitively it might seem that inter-branch accountability should be more robust than, say, intra-agency accountability (perhaps because branches are further removed from one another), this may not always be the case. Some have argued that separation of parties leads to more productive political debate than does mere separation of powers. To be sure, horizontal accountability, whether between branches, or between agencies within the executive branch, results in redundancy—as is the case with the overlapping functions performed by

84 Note that these aspects of accountability can be found in Schedler, supra note 81 (enforcement, monitoring, and justification), and Michaels, supra note 10 (gatekeeping, reporting, and reviewing). I focus on transparency rather than monitoring so as to include the concepts of reporting and auditing. Gatekeeping and enforcement are related, but distinct. Enforcement involves the use of sanctions (that is, negative consequences). Gatekeeping, as Michaels notes, usually involves requiring the government to supply certification such as a warrant or subpoena. Michaels, supra note 10. NSLs, however, present an interesting case because the point of NSLs is that there is no requirement of obtaining a warrant or grand jury subpoena. Each NSL authorizing statute merely requires certification that the information is requested pursuant to a national security investigation. Thus, gatekeeping is currently necessary to a limited extent in that recipient companies should require at least the bare showing of a certification. I contend, however, that some added enforcement mechanism is necessary.

85 See Larry Diamond, The Democratic Rollback: The Resurgence of the Predatory State, 87 FOREIGN AFF. 36, 44 (2008) (“Horizontal accountability invests some agencies of the state with the power and responsibility to monitor the conduct of their counterparts.”).


87 See Levinson & Pildes, supra note 79.
the two chambers of Congress. But the “friction” resulting from overlapping jurisdiction, mandatory review of government action, and reporting requirements, among other transparency measures, is indeed an intended result.

Although horizontal accountability is a hallmark of American government, national security letters present a special case. In an ordinary (non-national security) law enforcement investigation, the law would normally require ex ante approval and possibly ex post review of the FBI’s (or other law enforcement agency’s) request for information. For the law enforcement agency, ex ante approval would take the form of a warrant or a grand jury subpoena in order to seize documents with private information. Like any warrant, such a process would involve horizontal accountability. If the judiciary determines that the warrant lacks probable cause, the petition for warrant may be denied. The law enforcement agency would thus have to be relatively transparent in that it would have to reveal information supporting its decision to the judge. The agency would further have to justify its action by meeting the burden of probable cause.

National security letters, however, provide a special case. The whole point of the NSL statutes is to provide the FBI with a legitimate means of bypassing the warrant and grand jury subpoena requirements. Congress has determined that, in the context of national security investigations, certain types of requests may be urgent enough that the FBI should be able to act without going through the judiciary.

There is another way in which the FBI is not accountable to the judiciary for its use of national security letters. Whereas the exclusionary rule of criminal procedure bars the admission of improperly obtained evidence—even if that evidence appears to be uncontradicted and verifiable—there is no analogue to the exclusionary rule in the context of improperly obtained national security letters.

Particularly in the context of ECPA-NSLs, the NSL is really a threshold mechanism for obtaining information. Often the information that is obtained by national security letter is not directly admitted as evidence in a criminal trial. After all, ECPA-NSLs do not authorize retrieval of the substance of electronic communications—that is, the main text or subject headings of emails or the actual phone conversations—but rather authorize more transactional data such as email addresses and phone numbers with which an individual has communicated. Rather than being admitted directly to trial, NSL-derived information is

---

88 See Katyal, supra note 84, at 2324 (“Partially overlapping agency jurisdiction could create friction on issues before they are teed up to the President for decision.”).

89 See generally id.

90 For a description of the legislative history regarding the NSL authorization statutes, see Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004) (describing the rationale for the ECPA and other similar privacy statutes and the corresponding exception for NSL authorizing statutes).

91 See DANIEL J. SOLOVE, MARC ROTENBERG, & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 270 (2006) (“The SCA does not provide for an exclusionary rule.”).
frequently used to obtain a FISA warrant for wiretapping or the ability to otherwise access the substance of electronic communications. The FISA court, which operates in secrecy, does not review whether the information derived from NSLs was improperly obtained. Indeed, the FBI does not even keep track of whether data was obtained by NSL through a tagging mechanism. Since the FISA court does not employ an exclusionary rule with respect to information obtained by improperly issued NSLs, the grant of a FISA warrant allows the FBI to obtain much more information in an authorized manner. If any evidence ultimately does reach a criminal trial, the evidence will have likely been properly obtained under the auspices of the FISA warrant, even though the FISA warrant was supported by improperly obtained NSL-derived information. In effect, the FISA application serves to cleanse FBI’s misconduct.

Until recently, the FBI has additionally not had any significant accountability toward Congress or the other agencies of the executive branch for its use of NSLs. As I discuss in further detail in Part II.C, however, the Patriot Reauthorization Act took an important first step in providing horizontal accountability between the FBI and Congress and between the FBI and the Justice Department’s inspector general.

Thus, although the FBI is beginning to experience meaningful horizontal accountability with respect to Congress and the Office of the Inspector General, there is a unique absence of horizontal accountability between the FBI and the judiciary. While there is at least a plausible argument that imposing a warrant requirement would be overly burdensome, providing an analogue to the exclusionary rule for NSLs in the FISA court would probably not hinder effective investigation. Moreover, if the FBI were to ever seek to directly admit NSL-derived information into evidence in a criminal proceeding, I would further argue that the exclusionary rule should operate to deny NSL-derived information unless the FBI can demonstrate that the information was obtained properly. Of course, before any of this is possible, it would be necessary for the FBI to develop a procedure for tagging NSL-derived information.

This case is analogous to the idea that interrogators will be reluctant to use enhanced interrogation techniques if they fear that any testimony gained under

92 See OIG 2007 REPORT at xxiv (describing the most common uses of NSL-derived information and noting that “the most important use” of ECPA-NSLs “is to support FISA applications for electronic surveillance, physical searches, or pen register/trap and trace orders”).

93 See infra note 95.

94 This is not to say, however, that such accountability between the FBI and Congress and the OIG is sufficient. I argue below that such accountability is beneficial and should not be done away with. Other accountability measures that I suggest in this Comment should be considered as supplements to rather than replacements for currently existing accountability measures.

95 See discussion infra Part IV.C.

96 See infra note 95.
use of such techniques will be unavailable in court. Given that the FBI (as opposed to the CIA, which is more exclusively concerned with intelligence gathering) is highly concerned with not only intelligence gathering, but also the eventual prosecution as a result of investigation, this should be an effective incentive.\textsuperscript{97}

The main obstacle to this approach, however, is that under the current regime it would be difficult for FISA court judges to determine that information was obtained improperly. On the other hand, proving a violation of the Stored Communications Act should not be significantly more difficult than proving a similar violation under the Wiretapping Act, and yet the Wiretapping Act includes an exclusionary rule.\textsuperscript{98} Another significant problem here is that the FBI does not tag all information obtained by NSL.\textsuperscript{99}

Another obstacle stems from the proxy substitution problem. In a sense, my proposal suggests directing the FISA court to at least partially stand as a proxy for the American public. Ideally, we would like to have the FISA court invalidate information obtained improperly. Proxy substitution is limited, however, by various factors.\textsuperscript{100} FISA judges do not want to be the ones to prevent a critical element of protecting against a major national security problem. In fact, from 1978 through 2009, only a total of fourteen applications were denied out of a total of tens of thousands.\textsuperscript{101}

2. Vertical Accountability

National security letters also are significantly exempted from vertical accountability. Vertical accountability, which usually may refer to the accountability between government and the people by means of elections,\textsuperscript{102} is

\textsuperscript{97} See infra note 170 (discussing the federal government’s precautionary attitude in anticipation of the potential capture of Osama bin Laden).
\textsuperscript{98} 18 U.S.C. § 2515 (“Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence . . . if the disclosure of that information would be in violation of this chapter.”).
\textsuperscript{99} OIG 2007 REPORT at xxvii (“[I]nformation derived from [NSLs] is not required to be marked or tagged as coming from NSLs when it is entered in FBI databases or when it is shared with law enforcement authorities outside the FBI.”). In response to the OIG’s recommendation to begin a system of tagging NSL-derived information and at the direction of the Attorney General, in 2007 the Department’s Chief Privacy and Civil Liberties Officer convened a National Security Letter Working Group, which concluded that tagging of NSL-derived information was not feasible at the time. See OIG 2008 REPORT at 33–34.
\textsuperscript{100} See Note, supra note 78 (describing various limitations on proxy substitution, including trust).
\textsuperscript{101} On the other hand, this might be viewed as an improvement given that for many years not a single application was denied. See FISA Court Statistics, supra note 4.
\textsuperscript{102} See Larry Diamond, The Democratic Rollback: The Resurgence of the Predatory State, 87 FOREIGN AFF. 36, 44 (2008) (“The premier example of vertical accountability is a genuine democratic election.”). See also id. (“Other effective forms of vertical accountability include
usually possible in the context of monitoring law enforcement conduct by means of lawsuits directed against the government by the offended individuals.

Carrying forward the analogy to a non–national security investigation, there are some circumstances where even law enforcement officials may lawfully effect a seizure without first obtaining a warrant. The presence of exigent circumstances is one such exception.\[^{103}\] Even in such cases where ex ante approval is not required, however, law enforcement officials are still generally accountable to the individuals directly affected by the intrusion. If an individual feels that they have been wronged, such an individual is able to sue.\[^{104}\] Such a private cause of action provides an opportunity to the plaintiff to vindicate his or her rights and also acts to deter the law enforcement official from improper behavior. As opposed to ex ante approval through a warrant, a private cause of action provides for an additional element of accountability—enforcement.

In the context of NSLs, enforcement in court is severely restricted by a number of causes. First, the combination of the gag order on NSL recipients and the secrecy of national security investigations makes it highly unlikely that affected individuals will ever know about the information retrieval. Moreover, even if individuals do discover the information retrieval, the remedies in court are unclear.

In sum, the FBI’s use of NSLs substantially lacks in either horizontal or vertical accountability.

3. The Inherent Costs of Accountability

Although accountability creates positive externalities such as legitimacy and compliance, there are inherent costs of accountability as well. First, approval requirements (such as the warrant requirement for law enforcement) slow down law enforcement. In perilous circumstances, warrants cost time and time may even cost human lives. Although the approval process may be streamlined, the warrant requirement means that it will take longer for law enforcement officials to, for example, carry out a search. Also, all of the time and effort that is used to obtain a warrant is time and effort that could be used on some other investigation.

Transparency also imposes costs in the law enforcement context. Similar to approval mechanisms such as the warrant requirement, transparency can have
an ossifying effect on agency action. Additionally, audits may create a substantial burden for law enforcement agencies. For example, the OIG’s audit of the FBI’s use of NSLs required scores of interviews and the production of tens of thousands of documents such as national security letters and investigative case files, as well as “documentation pertaining to case initiations, authorizations, delivery to the designated recipients, the recipients’ production of documents and electronic media in response to the letters, retention of that information, and the analysis and dissemination of the information within the Department, to the intelligence community, and to others.”

In addition to the costs of accountability, it is also important to consider the limitations of accountability. Although enhancing certain kinds of accountability (through mechanisms such as those discussed in this Comment) is likely to improve compliance, are there still ways in which the transgressions or abuses may likely continue? Certainly mechanisms such as providing a private cause of action or establishing an exclusionary rule for data obtained in violation of the Stored Communications Act are underinclusive. Such inherent limitations can be reinforced, however, with supplemental accountability mechanisms such as periodic audits, as I discuss in further detail in Parts III and IV.

C. Accountability Resulting From the Reauthorization Act

In the USA PATRIOT Improvement and Reauthorization Act of 2005 (“Reauthorization Act”), Congress took an important step forward in establishing the FBI’s accountability for NSL usage by requiring the OIG to perform extensive audits of the FBI’s use of NSLs for the four-year period from 2003 to 2006. Before 2006, the Justice Department made no public reporting of NSL statistics.

The Reauthorization Act provided the first meaningful measure of horizontal accountability by providing much-needed transparency. The OIG Reports, which were made available to the public, provided detailed information

---

105 See Note, supra note 78, at 1556 (“Government often needs to operate in secret in order to shape and execute socially desirable policies, and excessive transparency requirements can have an ossifying effect that prevents government from responding in innovative ways to changed circumstances.”).
106 OIG 2007 REPORT at 3–5.
107 USA PATRIOT Improvement and Reauthorization Act, § 119(b) (see infra note 47).
108 Prior to the OIG audits, the FBI had been required to make classified semiannual reports to Congress reporting only the number of NSLs issued. It is relevant to note, however, that the OIG discovered significant underreporting to Congress. OIG 2007 REPORT at xvi (“[T]he total numbers of NSL requests that were reported to Congress semiannually in CYs 2003, 2004, and 2005 were significantly understated. . . . [W]e estimated that approximately 8,850 NSL requests, or 6 percent of NSL requests issued by the FBI during this period, were missing from the database.”).
on many aspects of the FBI’s use of national security letters. The OIG Reports
detail the types of violations and the magnitude of the problems that were found.
Furthermore, in each report, various recommendations were made.

In just a few years, the OIG Reports seem to have had an important impact
on the FBI’s use of national security letters. As reported by the OIG, the FBI
leadership’s reaction to the OIG’s recommendations was apparently positive.
Indeed, the FBI even labored to develop its own set of internal recommendations
in order to go above and beyond the recommendations of the OIG. With some of
the OIG’s recommendations, however, the FBI gave some resistance. For
example, the FBI was opposed to the OIG’s recommendation to tag all
information obtained by NSLs.\textsuperscript{109}

Each of the reports, in addition to uncovering various types of improper
behavior with regard to the use of the FBI’s NSL authority, also provided
recommendations to the FBI.\textsuperscript{110} In its 2008 report, the OIG noted that the FBI
had clearly made important and significant efforts to begin to implement various
of the OIG’s recommendations.\textsuperscript{111}

In addition to accountability measures already set in place by Congress,
three bills, under consideration in the 111th Congress, contained various
provisions that (together, at least) would have improved accountability for the use
of NSLs. The three bills—H.R. 1800 (Nadler), S. 1682 (Leahy), and S. 1686
(Feingold)—addressed various aspects of the NSL statutes such as the standard
for issuance, the scope of covered records, judicial review of NSL requests,
issuance and judicial review of gag orders, a private right of action, public
reporting and audits, and a sunset provision.\textsuperscript{112} Each of the bills expired at the
close of the 111th Congress, and it remains to be seen when and how similar
proposals will resurface.

D. Are the Recent Improvements Enough?

Despite both the important advances that Congress has provided and will
likely continue to provide and the OIG recommendations, more can and should be

\footnotesize{109} See supra note 99.

\footnotesize{110} For example, in the 2007 Report, the OIG made ten recommendations, including, among other
recommendations, requiring all authorized issuers of NSLs to create a control file to retain signed
copies of all issued NSLs, considering measures that would enable tagging of NSL-derived
information, and taking measures to reduce the improper use of exigent letters and to comply with
existing NSL statutes. OIG 2007 REPORT at xlix.

\footnotesize{111} See OIG 2008 REPORT at 8 (“[W]e believe the FBI and the Department have evidenced a
commitment to correcting the problems we found in our first NSL report and have made
significant progress in addressing the need to improve compliance in the FBI’s use of NSLs.”).

\footnotesize{112} For a description of each of the bills, see source cited in note 116, infra.
done to enhance the FBI’s accountability for the use of NSLs. As the Office of the Inspector General reported in its 2008 report:

[...]We believe that ensuring full compliance will require the continual attention, vigilance, and reinforcement by the FBI and the Department. We also believe it is too soon to definitively state whether the new systems and controls developed by the FBI and the Department will eliminate fully the problems with the use of NSLs that we and the FBI have identified.\(^{113}\)

While the OIG’s recommendations will likely reduce the number of improperly issued NSLs, particularly where the impropriety is the result of mistake, many of the recommendations do not enhance external accountability and are merely self-enforcement mechanisms. Moreover, if we care not only about deterring misconduct, but about compensating the individuals that have been harmed, the OIG’s recommendations are inadequate.

Similarly, while the three bills previously under consideration sought to increase the FBI’s answerability for NSL usage, there was only one provision that provided for enforcement. This provision,\(^{114}\) which would have created a private cause of action, is something that I also propose in Part III. I argue, however, that a private cause of action can only be made effective if supplemented with provisions that would enable affected individuals to learn of violations.

### III. Creating an Effective Private Cause of Action

In this Part, I discuss how a private cause of action can be designed in order to enhance the FBI’s accountability for the use of NSLs. Although the Patriot Reauthorization Act provided NSL recipients—for example, the telecommunications providers of individuals under investigation—with the ability to challenge a gag order or the NSL itself, the recipient companies are not sufficiently encouraged to expend time and money in defense of their customers’ privacy.

I begin by describing the current scheme under the ECPA. I demonstrate that the ECPA provides no private cause of action (explicitly, at least) against the FBI, and provides, at most, a very limited avenue for suing telecommunications providers. I then sketch the basic contours of a private cause of action for the aggrieved individuals (the individuals whose information is targeted by NSLs), borrowing from a now expired bill making a similar proposal.\(^{115}\) Given, however, that such a private cause of action does little good if the NSL target never knows about the NSL, I further suggest various means by which delayed disclosure may enable potential plaintiffs to learn of the retrieval of their records.

---

\(^{113}\) OIG 2008 REPORT at 15.

\(^{114}\) See infra note 114.

\(^{115}\) See infra note 125.
A. Protections Currently Available Under the ECPA

Currently, there is no explicit private right of action specifically for NSLs. Although the ECPA and other privacy statutes establish a private right of action for improper production of private customer information, it is unclear at best whether such rights of action would meaningfully benefit NSL targets.116

Title II of the ECPA, also known as the Stored Communications Act (SCA), regulates disclosures of subscriber information by telecommunications providers.117 Sections 2702 and 2703 provide the grounds for violations, whereas sections 2707 and 2712 provide the remedy for violations in the form of a civil action.118 As I will discuss immediately below, the core problem is that it is ambiguous at best whether improper retrieval of information with an NSL or similar device by the FBI is a violation of the SCA.119

It is also important to mention that section 2709, the specific section of the SCA authorizing the use of an ECPA NSL, does not by itself explicitly provide grounds for a violation of the SCA (as do sections 2702 and 2703). 2709(a) first places upon the NSL recipient the duty to comply with a request made under subsection (b). Subsection (b) then provides that authorized NSL issuers “may” request certain subscriber information, toll billing records, and electronic communication transactional records upon certification that the “records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation

---


118 18 U.S.C. § 2702 (setting forth grounds for violations regarding voluntary disclosures), 2703 (providing grounds for violations regarding disclosures compelled by the government), 2707 (providing a civil cause of action), 2712 (providing a civil cause of action against the United States). Although the civil action against the United States might appear to provide a civil action against the FBI for improper use of its NSL authority, as I discuss below, it is unclear whether any section provides grounds for violations of the SCA against governmental entities. Section 2712 may be reconciled under the interpretation that it covers cases where the federal government (like a telecommunications provider) improperly discloses information protected under the SCA.

119 See Orin S. Kerr, A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It, 72 GEO. WASH. L. REV. 1208, 1242 (2004) (noting that the SCA is “unclear as to when the government is liable for violating the statute, as opposed to the ISP, or both”).
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 . . . .”

A reasonable interpretation of the statute is that the certification requirement merely provides for the circumstances in which the NSL recipient is compelled to disclose information. On the other hand, the statute might be interpreted to read that the FBI may not request information if the FBI has not truthfully made the required certification. Given the ECPA’s purpose of protecting individuals’ private information, the latter interpretation seems to be the stronger.

Few courts have had opportunity to consider whether governmental entities in general may violate sections 2702 or 2703. There is a split in authority. In Tucker v. Waddell, the Fourth Circuit held that subpoenas that were improperly issued by police officers of Durham, North Carolina did not constitute a violation of section 2703(c) of the SCA because that section did not apply to the government. In Freedman v. American Online, however, a Connecticut district court rejected the approach taken in Tucker and held the government liable for failure to comply with section 2703(c). Scholars have generally sided with Freedman, while also acknowledging that the law needs to be clarified. Moreover, although section 2703 provides a possible grounds for bringing a private action against NSL recipients, telecommunications providers have been afforded broad leeway given the good-faith complete defense contained in section 2707(e).

Thus, the current scheme is insufficient because it does not provide a clear remedy for offended parties. Setting aside the question of how the aggrieved individual may learn of the FBI’s retrieval of their private information, deterring improper behavior by the FBI through the use of a private cause of action may only be successful if the cause of action is clearly available. More importantly, even if NSL targets did have a clear private right of action against the FBI for misuse of an NSL, under the current scheme few, if any, NSL targets would ever know about it. The vast majority of NSLs contain gag orders.

Thus, the current scheme is insufficient because it does not provide a clear remedy for offended parties. Setting aside the question of how the aggrieved individual may learn of the FBI’s retrieval of their private information, deterring improper behavior by the FBI through the use of a private cause of action may only be successful if the cause of action is clearly available. More importantly, even if NSL targets did have a clear private right of action against the FBI for misuse of an NSL, under the current scheme few, if any, NSL targets would ever know about it. The vast majority of NSLs contain gag orders.


\[121\] See Freedman, 325 F.Supp.2d 638; Kerr, supra note 103. The reasoning is that it would not make sense to place limitations on the government’s ability to obtain data and to then permit the government to skirt those limitations with impunity.

\[122\] Tucker v. Waddell, 83 F.3d 688 (4th Cir. 1996); see also Kerr, supra note 119, at 1241 (noting that “[t]he reasoning in Tucker is weak” and that Freedman “has held that amendments to the SCA in the USA Patriot Act have overruled it”); Susan Freiwald, Online Surveillance: Remembering the Lessons of the Wiretap Act, 56 ALA. L. REV. 9, 59–60 (2004) (citing Guest v. Leis, 255 F.3d 325, 339 (6th Cir. 2001)) (noting that Tucker, which was affirmed by the Sixth Circuit in dicta, “stands as a stark example of how little privacy the courts are willing to read into the ECPA”).


\[124\] 18 U.S.C. 2707(e).

\[125\] See supra note 19.
such nondisclosure orders, even under recent amendments in the Patriot Reauthorization Act, allow the FBI to unilaterally determine whether the gag order is necessary, subject only to possible challenge by the NSL recipient in court.\footnote{See Jameel Jaffers Testimony, at 7 (“Gag orders imposed under the NSL statute are imposed by the FBI unilaterally, without prior judicial review. While the statute requires a ‘certification’ that the gag is necessary, the certification is not examined by anyone outside the executive branch. No judge considers, before the gag order is imposed, whether secrecy is necessary or whether the gag order is narrowly tailored.”).}

B. Proposed Cause of Action

Section 4 of H.R. 1800 (Nadler), proposed in 2009 (and expired at the end of the 111\textsuperscript{th} Congress at the end of 2010) created a cause of civil action for misuse of NSLs if the NSL “was unlawful or certification was without factual foundation.”\footnote{Section 4 of H.R. 1800 (Nadler) (2009).} The bill provided for the greater of $50,000 or actual damages.\footnote{\textit{Id.}} Consistent with Representative Nadler’s proposal, I also propose that a private cause of action be explicitly established. I would like to expand, however, on this idea by addressing the basic contours of such a cause of action.

Under my proposal, the plaintiff would be the individual or individuals whose records were obtained by NSL (as the SCA refers to them, the “aggrieved individuals”). This proposal thus differs from the existing NSL-authorizing statute, which enables only the NSL recipient to challenge aspects of the NSL in court. The proper defendants should be the FBI personnel issuing the NSL, in addition to the FBI, the Department of Justice, and the United States.

The amendment could be implemented by various means. One approach would be to amend section 2709 to explicitly state the grounds for violation by the FBI—such as improper use of an exigent letter, issuance of an NSL without the required certification or authorization, or failure to properly file an approval electronic communication. The amendment to section 2709 could be supplemented by an amendment to 2712 that would explicitly include violations of the grounds set forth in section 2709.

A broader approach would be to amend sections 2702 and 2703 to explicitly provide that governmental entities, in addition to telecommunications providers, may violate the provisions of the sections upon improperly seeking either voluntary or compulsory disclosure. Proper issuance of an NSL should then be included as an exception—among other exceptions—to the general
requirement that governmental entities may not obtain private information protected under the SCA.  

C. Delayed Declassification

The primary obstacle to successfully using a private cause of action to increase accountability of NSL-issuing personnel is that aggrieved individuals usually never know about the violation of their privacy rights. Thus far, challenges in court to the FBI’s issuance of NSLs, have focused on the free speech concerns of the recipient entities (for example, a telecommunications provider that receives the NSL request) and not on the privacy rights involved with the targets of NSL requests. Although the landscape is now much clearer with respect to what rights recipient entities have to challenge NSL requests, the existence of the gag order leaves open the question of how to adequately protect the privacy rights of the NSL targets.

Thus, the question is how to enable the targets of NSLs to learn of the improper use of NSLs to target their own personal information. This question is made particularly difficult by the great value of secrecy in national security investigations. To say that secrecy is an essential element of national security investigations, however, is not to say that disclosure should be completely blocked. A hybrid solution is possible, one that balances the costs and benefits of accountability, on the one hand, with the need for secrecy on the other. The solution that I propose is a provision for delayed disclosure or declassification.

Perhaps the most workable mechanism for disclosure is to provide for a lifting of

129 Note, however, that this solution would still leave open the question of how to enable potential plaintiffs to learn of potential violations.

130 See Erwin Chemerinsky, Essay: Civil Liberties and the War on Terror: Seven Years After 9/11 History Repeating: Due Process, Torture and Privacy During the War on Terror, 62 SMU L. REV. 3, 12 (2009) (“[W]hen government actions are shrouded in secrecy, the problem that arises is that we can lose our privacy and not even realize it.”).

131 See Doe v. Gonzales; see also Nathan Alexander Sales, Secrecy and National Security Investigations, 58 ALA. L. REV. 811, 813 (2007) (“Not only are third parties effectively conscripted into participating in the government’s national security operations, but they also will find themselves forbidden from speaking about their interactions with investigators. And those restrictions put a real strain on free speech, privacy, and other constitutional values.”).

132 See generally Note, supra note 78, at 1574–77. There is already a process in place for the general declassification of documents. See OIG 2007 REPORT (“Security-classified documents may become declassified if a date or event for declassification, prescribed at the time of their classification, is realized; an applicable time frame, such as 10 years or, by extension, 25 years, from the date of original classification, lapses; an authorized holder of the classified documents successfully challenges the continued need for their protected status; or a mandatory review by agency officials, prompted by a request pursuant to the President’s security classification executive order or the access procedures of the Freedom of Information (FOI) Act, results in a determination that classification is no longer warranted.”).
the gag order imposed on NSL recipients after a certain amount of time, thus permitting (or perhaps requiring) the NSL recipients to notify their customers of the retrieval of their information.\(^\text{133}\) Placing the decision of disclosure on the NSL recipients provides a way that NSL targets can learn of improper NSL use, without burdening the FBI or the U.S. government with an affirmative disclosure obligation.\(^\text{134}\) The individuals would then be able to make a FOIA request to have records of the initial NSL request in addition to the information actually received by the FBI.

To be effective, disclosure of information would have to make available enough information that harmed individuals would be able to know that their information had been targeted and that the information had been obtained improperly. Although the NSL recipient is often not apprised of the specific reasons why a given customer’s information is being targeted, such reasons should be found in the approval electronic communication (approval EC) that is initially used to gain approval to issue the NSL. Every NSL requires an approval EC.\(^\text{135}\) The individual making the request should also be able to request a list of records actually obtained.

Furthermore, the disclosure would have to be timely.\(^\text{136}\) Disclosure would have to be timed so as not to create too great of costs by revealing too much information while national security investigations are still open. Thus, one

\(^{133}\) An analogy here may be drawn to the various laws requiring affirmative disclosure of data security breaches. See, e.g., Cal. Civ. Code § 1798.82(a) (“Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.”); see generally Stewart Room, Presentation: “Breach Disclosure and Cloud Computing: Everything You Need to Know About the EU’s Position on Breach Disclosure,” September 2010, http://www.stewartroom.com/wp-content/uploads/2010/10/Breach-Disclosure-in-Europe-and-Impact-for-Cloud-Computing-Webinar-10-September-2010ppt.ppt (podcast presentation slides) (surveying breach disclosure laws and proposals in the United States and Europe).

\(^{134}\) This solution falls somewhere between declassification and disclosure by the government. Declassification does not equate to public availability; declassified files may still be publicly withheld. Placing an affirmative obligation to disclose on the U.S. government would be cumbersome given the sheer number of NSLs issued and would further present a significant conflict of interest, given the potential embarrassment and vulnerability to damage suits. See infra note 158 and accompanying text.

\(^{135}\) See infra note 78, at 1574–77 (“If the delay is calibrated properly, this strategy could both give government officials the ability to take socially desirable action that would be difficult without secrecy and provide them with the appropriate incentives not to act out of self-interest.”).
possible option would be to provide for mandatory disclosure once cases are closed. This solution, however, would still leave ultimate discretion in the hands of the FBI agents for the particular case. The incentive under such a solution would clearly be for FBI agents to not close any cases.\textsuperscript{137}

There are two potential solutions to this problem, both involving review by another government agency. First, rather than delaying disclosure until the closing of the relevant investigation, a mandatory period of time—say, three years—could be imposed, within which the FBI must either disclose the information or obtain external approval to keep the case open or the information secret (even if the case itself is closed). This would be similar to the more general strategy of the federal government with respect to classified materials. In 1995, President Clinton signed an executive order that mandated declassification of classified records more than twenty-five years old, with some exceptions.\textsuperscript{138} In order to keep the information secret, the FBI would have an escalated burden of proof\textsuperscript{139}—rather than merely showing that the information was relevant to a national security investigation (which is the certification requirement for issuance of an NSL under Section 505 of the PATRIOT Act), the FBI should have to—for example—provide evidence indicating the harm likely to come about upon disclosure of the specific information.\textsuperscript{140}

Thus, for example, suppose that the FBI rightfully initiates an investigation of an individual and obtains a lead indicating that the person is connected with a known terrorist organization. Following up on the lead, the FBI issues various NSLs to obtain a variety of information about the individual.\textsuperscript{141} If three years after the issuance of the NSLs, the FBI considers that allowing the NSL recipients to inform the individual of the NSL requests would raise serious national security problems, perhaps out of the concern that doing so would alert the terrorist organization of the extent of the FBI’s investigation, the FBI may seek reauthorization of the nondisclosure order from the FISA Court. In order to

\textsuperscript{137} Concerns about overclassification and delayed declassification have been expressed on many occasions. See Lawrence J. Halloran, Briefing Memorandum for the hearing, Emerging Threats: Overclassification and Pseudo-classification, available at http://www.fas.org/sgp/congress/2005/halloran.pdf.

\textsuperscript{138} Exec. Order No. 12,958, 3 C.F.R. 333 (1996); Note, supra note 78, at 1576.

\textsuperscript{139} See Michaels, supra note 10, at 951 (proposing a reform “mandating . . . escalating burdens of proof that require agencies periodically to demonstrate to the FISA Court the continuing utility of ongoing operations”).

\textsuperscript{140} Cf id. at 964 (arguing that the FISA Court should have to review and reauthorize surveillance programs by “evaluat[ing] briefings on the evidentiary support justifying the program, the utility of the information obtained as weighed against the invasiveness of the inquiries, and the potential for false positive identifications (and the harms that those false positives spawn)”). My proposal could be viewed as a specific and scaled-down implementation of Michaels’s proposal.

\textsuperscript{141} This scenario may be more or less ordinary as far as NSLs go. For some generic examples of the types of uses for NSLs, see OIG 2007 REPORT at 49.
do so, the FBI would have to articulate facts supporting its contention that a lifting of the gag order would endanger lives or an ongoing national security investigation.

A second approach would be to have an agency of the federal government review the FBI’s open investigations in order to determine whether cases were being held open improperly. Perhaps the role of the Justice Department’s Inspector General could be expanded to perform this function. This approach would be at least consistent with the requirement that information should not be classified merely to avoid embarrassment or cover-ups. This approach would be more deferential to the FBI because the FBI would not have to make an affirmative determination for each NSL.

There are certainly costs to and concerns with this approach. Clearly such oversight would involve administrative costs. In essence, taxpayers would be paying to police the FBI’s actions. More importantly, the value of having external entities such as the FISA Court or the OIG determine whether the gag order should be retained or whether the FBI is improperly leaving cases open depends largely on the degree to which we trust such entities to make determinations that are representative of the will of the American public. Since the FISA Court itself operates in secrecy, there is a concern that the FISA Court will err too much on the side of taking the FBI’s word, without a searching inquiry into whether the FBI is truly acting appropriately. Indeed the FISA Court has rejected extremely few applications for warrants. On the other hand, although it is hard to tell with any certainty, perhaps the low rejection rate for FISA applications is in part a result of the successful deterrence that the FISA Court imposes. Similarly, the hope is that the delayed disclosure would at the very least deter the FBI from the most egregious abuses of NSL authority. Moreover, this concern could potentially be mitigated by a requirement that the briefing produced by the FBI as well as the FISA Court’s transcript or Inspector General’s report be made available under seal to Congress or other relevant agencies.

In conclusion, I have argued in this Part that by clarifying the availability of a private cause of action for violations of the SCA by the FBI in exercising its NSL authority and providing a delayed disclosure regime with a mechanism for

---

142 See supra note 138.
143 See Note, supra note 78 (noting that distrust is a limiting factor on the effectiveness of proxy substitution).
144 See FISA Court Statistics, supra note 4 (reporting that in 2009 only one out of 1320 FISA applications was rejected).
145 See Michaels, supra note 10, at 965 (“Regardless of the outcome, and in the interest of ensuring inter-branch dialogue, the briefing papers and a copy of the FISA Court’s transcript should be delivered under seal to the congressional oversight committees and to the relevant inspector general.”).
reviewing or auditing the FBI’s discretion to declassify, the FBI will be more accountable for the use of its NSL authority.

IV. AN EXCLUSIONARY RULE FOR NSLS

National security letters are a means to an end. In fact, NSLS usually are used early in the FBI’s investigatory process. Of the various purposes that NSLS serve, a key purpose is to gather evidence that may either be used in support of a FISA application or in a criminal prosecution. FISA applications for warrants enable the FBI to take information gathering at the NSL stage to the next level.\textsuperscript{146} Under the ECPA, NSLS allow the FBI to gain access to the nonsubstantive information about electronic communications such as email recipients and senders.\textsuperscript{147} If the FBI discovers suspicious links as a result of information gathered via national security letters, the next step is to discover the substance of the emails by submitting a FISA application for wiretapping or other investigatory tools. Although less common (perhaps because of the fact that better evidence may be obtained after obtaining a FISA order), NSL-derived information may likewise be used as evidence in a criminal prosecution.\textsuperscript{148}

In this Part, I propose the establishment of an exclusionary rule,\textsuperscript{149} designed to bar the admission of information obtained improperly under the FBI’s NSL authority.

A. Suppression in the FISA Court and in Criminal Proceedings

The defining attribute of the FISA Court is that it operates in secrecy.\textsuperscript{150} If evidence is introduced in a criminal trial that was obtained as a result of a FISA

\textsuperscript{146} See OIG 2007 REPORT at xxiv (noting that “the most important use” of ECPA-NSLS “is to support FISA applications for electronic surveillance, physical searches, or pen register/trap and trace orders”).

\textsuperscript{147} See id. at xxiv (“FISA court orders for electronic surveillance may authorize the FBI to collect the content of telephone calls and Internet e-mail messages, information the FBI cannot obtain using NSLS.”).

\textsuperscript{148} Among the “principal objectives for using NSLS” reported by FBI personnel is the objective to “develop information that is provided to law enforcement authorities for use in criminal proceedings.” Id. at xxii.


\textsuperscript{150} See Daniel J. Solove, Marc Rotenberg, & Paul M. Schwartz, \textit{Information Privacy Law} 289 (2006) (“[FISA Court] proceedings are ex parte, with the Department of Justice (DOJ) making the applications to the court on behalf of the CIA and other agencies. The Court meets in secret and its proceedings are generally not revealed to the public or to the targets of the surveillance.”); Erwin Chemerinsky, \textit{Civil Liberties and the War on Terrorism}, 45 WASHBURN
order, the defendant is unable to learn of the basis for the grant of the FISA order. The problem is that there is currently no exclusionary rule regarding the use of information improperly obtained under the FBI’s NSL authority in hearings before the FISA Court. The FBI may rely upon information gathered by NSLs even if the information was obtained improperly and even if the FBI should never have been able to legally access the information. Since FISA Court proceedings are necessarily ex parte, the individual under investigation cannot move to suppress NSL-derived information (or any information for that matter) during the FISA Court briefings. If information improperly obtained under the FBI’s NSL authority is used to obtain a FISA order that is then used properly, the grant of the FISA application effectively cleanses the FBI’s improper conduct with regard to the issuance of the original NSL. Thus, the violation of privacy interests resulting from the improper receipt of private information from NSLs is compounded when that same improperly obtained information is used more or less as evidence to support the gathering of much more information.

Similarly, there is no explicit exclusionary rule under the SCA, which contains the authorization for ECPA NSLs, for civil or criminal trials. Some decisions, however, have suppressed information obtained by state or local governmental entities in violation of section 2703 of the ECPA, thus implicitly using an exclusionary rule.

---

151 L.J. 1, 16 (2005) (“A key aspect of [FISA] is that it relaxes the usual probable cause standard followed under the Fourth Amendment. The Act provides that an order can be issued if there is ‘probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power.’ . . . FISA provides that individuals may not have access to information obtained under a FISA warrant. In response to a suppression motion, the judge makes an in camera and ex parte review to decide whether suppression is warranted. The defendant is not allowed to see the basis for the FISA warrant when making a suppression motion. As originally enacted, FISA applied only to electronic surveillance, but was amended in 1995 to include physical searches.” (citations omitted)).

152 See DANIEL J. SOLOVE, MARC ROTENBERG, & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 270 (2006) (“The SCA does not provide for an exclusionary rule.”); id. at (noting also that, in contrast to the SCA (Title II of the ECPA), the Wiretap Act (Title I of the ECPA) does contain an exclusionary rule); see also Jon D. Michaels, All the President’s Spies: Private-Public Intelligence Partnerships in the War on Terror, 96 CAL. L. REV. 901, 949 (2008) (“[B]ecause national-security investigations usually do not lead to regular, criminal trials but instead to detentions, deportations, or just further investigations (with the aim of catching the principals overseas in a military operation), there is no . . . deterrent on the U.S. intelligence agents [comparable to suppression hearings before an Article III judge].”).


154 See Freedman, 325 F.Supp.2d 638.
B. An Exclusionary Rule for NSL-Derived Information

This proposal would require FISA Court judges to scrutinize the propriety of NSL-derived information sua sponte. Essentially, the FBI would be required to demonstrate how it obtained its evidence, used in support of the FISA application. If NSLs were used to obtain information, the FBI will have to demonstrate that NSLs were used properly. The main difference in a criminal trial is that the defendant will be able to move to suppress evidence that was obtained improperly under the FBI’s NSL authority. If the prosecution (or the FBI) believes that the details regarding the issuance of the NSLs should be disclosed to the defendant, the judge should be able to consider the FBI’s briefing on the manner in which information was obtained and approval sought in camera.

If the judge reviewing the evidence determines that information was obtained improperly—for example, as a result of an improperly issued exigent letter—the judge should bar the consideration of such information in the determination of whether to issue a FISA order or, if in a criminal proceeding, should deny admission of the evidence at trial. This of course would not prohibit the introduction of other properly obtained information in order to reach the same end.

Although NSL-derived information is undoubtedly used internally in many circumstances, the key to the proposed exclusionary rule is to make the FBI accountable at least in the subset of cases where it may seek to make external use of information obtained from NSLs. For example, the FBI may seek to use information obtained as a result of issuing an NSL in order to support FISA applications or in order to corroborate other evidence in a criminal proceeding. While it is true that much of the information collected by the FBI is not subject to after-the-fact checks by a judge, many times the FBI will not know what it will want to use the information for until after it requests the information because the NSL is generally used early in the investigatory process. Thus, the threat that useful information will be unavailable under certain circumstances will serve as a partial incentive to issue NSLS properly.156

155 See OIG 2007 REPORT at 159 ("National security letters have various uses, including obtaining evidence to support Foreign Intelligence Surveillance Act applications for electronic surveillance, pen register/trap and trace devices, or physical searches; developing communication or financial links between subjects of FBI investigations and between those subjects and others; providing evidence to initiate new investigations, expand investigations, or enable agents to close investigations; provide investigative leads; and corroborating information obtained by other investigative techniques."); id. at 48 ("ECPA national security letters for subscriber information routinely are used to confirm [a] required element and to otherwise develop evidence to support orders from the FISA Court.").

156 See discussion regarding United States v. Ghailani in Part IV.C.
C. Obstacles to the Implementation of the Exclusionary Rule

One important obstacle to this approach derives from the technical complexity of the task. Depending on the amount of NSL-derived information being used, this approach could impose a heavy burden of production on the FBI, as well as a difficult task for the judges on the FISA Court (or other court considering the admission of NSL-derived information). In some circumstances, defects may be easy to identify. For example, in Freedman, police officers issued a subpoena without a judge’s signature, and the recipient company then complied with the improperly issued subpoena. In other circumstances, the FBI might issue an exigent letter or an informal request; the defect might be that the FBI agents do not prepare the necessary documentation required by the Attorney General Guidelines necessary to properly obtain a NSL; or the defect might be that the relevance of the information sought might be too attenuated.

In order for this approach to be effective, the FBI would have to develop a method for tagging NSL-derived information. As was recommended by the OIG, the FBI could possibly develop an automated system for tracking responses to NSLs, linked to any documents used to prepare the NSL, especially the Electronic Communication (EC) used to obtain approval of NSLs.

Although such substantiation requirements would increase FBI accountability and lead to increased compliance with NSL statutes, I admit that such an approach would be underinclusive. In some circumstances, FBI personnel could weigh the benefits of quickly receiving desired information against the expected cost of potentially not being able to use the information externally. Thus, the FBI under some circumstances could potentially take calculated risks after deciding that the expected benefits are greater than the expected costs.

On the other hand, this same argument has been deemed unavailing with respect to the use of the exclusionary rule in general. Moreover, a direct analogy

---

157 Freedman, 325 F.Supp.2d 638.
158 For a description of this and various other common potential defects, see supra Part I.D.
159 See OIG 2007 REPORT at 27 (“We found that the FBI has no uniform system for tracking responses to national security letters, either manually or electronically.”).
160 See OIG 2007 REPORT at 23 (explaining that the EC used to obtain approval of NSLs serves, among other functions, to “document[] the predication for the national security letter by stating why the information was relevant to an authorized investigation [and] documents the approval of the national security letter by appropriate personnel”). In addition to the NSL itself, the EC is the document that FBI administrative policy requires case agents to prepare in order to obtain an NSL. Id. For NSLs generated by FBI Headquarters, there is a parallel approval requirement. Id. at 24.
161 See Jon D. Michaels, All the President’s Spies: Private-Public Intelligence Partnerships in the War on Terror, 96 Cal. L. Rev. 901, 907 (2008) (“[T]he Executive is institutionally predisposed to act decisively and unilaterally during times of crisis, even if that means bypassing legal restrictions, skirting congressional and judicial oversight, and encroaching on civil liberties.”).
may be drawn to the context of excluding evidence obtained as a result of so-called enhanced interrogation techniques. For example, in *United States v. Ghailani*, the Southern District of New York excluded evidence obtained from Hussein Abebe in the course of the CIA’s use of enhanced interrogation techniques. The court there concluded that the testimony should be suppressed in accordance with “the basic principles that govern our nation,” notwithstanding that “perceived expediency [may] tempt[] some to pursue a different course.”

Similar to the context of suppressing evidence obtained as a result of enhanced interrogation, this proposal would potentially prevent some national security investigations from going forward. In times of war, always present is the question of how to balance national security and civil liberties. FISA Court judges may not want to be the one to prevent the use of a critical element of protecting against a major national security threat. The mere fact that the FBI is accountable, however, may be enough to at least partially deter improper conduct.

In sum, I have proposed the adoption of an exclusionary rule for evidence obtained in violation of the SCA. This would not only apply to the FBI’s use of NSLs, but would further resolve ambiguity in the SCA that has troubled courts such as in *Freedman* (in the local law enforcement context). I have noted some of the obstacles to the success of such an exclusionary rule; however, I have argued that these obstacles principally indicate the underinclusive nature of exclusionary rules in general. Furthermore, although there is a concern that there may be legitimate national security investigations that are stopped from going forward (similar to the effect of an exclusionary rule in the local law enforcement context), this overinclusiveness should be mitigated by the deterrent effect of the exclusionary rule. Although the stakes may be higher in the context of NSLs (in comparison to violations of the SCA by local law enforcement), the benefits in terms of increased protection of civil liberties should outweigh the mitigated costs. Such benefits are especially acute given that the targets of NSLs are unable to advocate their own interests since FISA Court proceedings are generally not open to them.

---

163 Id. at 68.
164 See, e.g., Erwin Chemerinsky, Essay: Civil Liberties and the War on Terror: Seven Years After 9/11 History Repeating: Due Process, Torture and Privacy During the War on Terror, 62 SMU L. Rev. 3, 3–4 (2009) (tracing the repression of basic civil liberties through U.S. historical events such as the passage of the Sedition Act in 1798, the Civil War, World War I, and beyond). See id. at 3 (“Throughout American history, the response to crisis, especially a foreign-based crisis, has been repression.”).
CONCLUSION

A remaining question is whether these proposals, in spite of their benefits, are likely to gain traction in Congress. Efforts to limit the executive branch’s national security investigatory tools have had limited success.\textsuperscript{165} Of all of the proposals, delayed declassification would likely face the greatest pushback. For one thing, an interesting aspect of declassification law is that it has developed through executive orders rather than statutes.\textsuperscript{166} More importantly, some may consider that the threat of revealing sensitive information, even if mitigated by providing the FBI with the ability to selectively shield certain investigations, is too great to risk. In this regard, the legislation can be made more palatable by not placing an escalated burden on the FBI to prove why particular cases should be left open. Instead, the OIG could be tasked with regularly auditing a sample of open case files to ensure that the FBI is generally keeping investigations open when necessary. Although this approach is underinclusive, it would be overall less cumbersome and probably more politically palatable. In contrast, my sense is that amending the Stored Communications Act to include an exclusionary rule would receive relatively less political resistance given that there is already an exclusionary rule in the Wiretap Act. Implementing an exclusionary rule, as I suggest above, would be more difficult in the FISA Court because of a variety of factors, including the low rejection rate of FISA Court requests and the high stakes involved.

If implemented, these mechanisms would likely increase compliance. In other domains in which transparency and accountability are limited, efforts to impose greater costs on the executive have resulted in improvements. Congress’s changed stance with regard to covert operations in the post-Iran-Contra era is one example. Despite the lack of any requirement that the CIA must consult the legislative branch in the National Security Act,\textsuperscript{167} Congress has subsequently

\textsuperscript{165} For example, with respect to the FBI’s NSL authority, each of the three bills proposed during the 112th Congress to amend the NSL statutes was not adopted. While the Patriot Reauthorization Act did create accountability in the form of an audit carried out by the OIG, the OIG gave recommendations, which the FBI is presumably free to accept or reject. See Letter, Robert S. Mueller, III at 1 (“It is important to note that the OIG found no intentional or deliberate misuse of these authorities but highlighted several areas where we must increase our audit and oversight of these tools.”) (emphasis added), OIG 2007 REPORT [hereinafter Mueller Letter]. Of course, FBI leadership seems to have embraced many of the OIG’s recommendations. See Mueller Letter (expressing agreement with respect to most of the OIG’s recommendations, though silent on certain recommendations). But, as I have argued, the OIG’s recommendations, even if adopted, would not foster increased accountability in the future.

\textsuperscript{166} See Halloran, supra note 137, at 3 (“Since 1940, classification of official secrets has been governed by policies and procedures flowing from executive orders of the President.”).

employed various measures to enhance accountability with respect to covert operations, including imposing congressional oversight and reporting requirements and punitive appropriations measures.\textsuperscript{168} As a recent example, perhaps in part as a result of cases like \textit{Ghailani},\textsuperscript{169} government officials were reportedly very cautious about the manner in which evidence might be obtained in anticipation of the potential capture of Osama bin Laden.\textsuperscript{170}

It is becoming increasingly apparent that privacy statutes such as the ECPA are not keeping pace with the times. Rather than attempting to answer the question of how the reach of the FBI’s NSL authority might be modified, this Comment takes a different approach by attempting to answer how the system may better hold the FBI accountable for its use of the NSL authority. It is clearly no easy task to enhance the FBI’s accountability for its use of NSLs. Simply put, secrecy and transparency don’t mesh well. While I concede that there may be costs to this Comment’s proposals, I believe that my approach mitigates such costs to the extent that, on balance, the proposals will create a net benefit.

\begin{footnotesize}
\begin{enumerate}
\item[169] See supra Part IV.C.
\item[170] Barbara Starr, \textit{U.S. Was Prepared to Fight Pakistani Forces, Officials Say}, CNN.COM (May 11, 2011, 4:25 AM), http://www.cnn.com/2011/WORLD/asiapcf/05/10/pakistan.us.military.fight/index.html?ref=rss_topstories&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed\%3A+rss%2Fcnn_topstories+%28RSS%3A+Top+Stories%29 ("The plan was for bin Laden to be flown back to Afghanistan aboard U.S. military helicopters and then flown out to the USS Carl Vinson in the north Arabian Sea. There was a team of lawyers, medical personnel, interrogators and translators standing by to deal with bin Laden if that was the scenario that unfolded. A major concern was to immediately ‘preserve evidence’ and put bin Laden into a legal framework that would ensure he could be charged and tried some day, the official said. ‘We didn’t want to have some case thrown out on a technicality.’")
\end{enumerate}
\end{footnotesize}