Chapter 1

The Need for a Practical Guide for Legal Counsel on Responding to National Security Letters

“FBI Headquarters and field personnel reported that they continue to believe national security letters are indispensable investigative tools that serve as building blocks in many counterterrorism and counterintelligence investigations.” — Department of Justice Office of the Inspector General, March 2008

“The FBI has been given too much power and is abusing it to stockpile massive databases on innocent Americans. . . . In fact, . . . hundreds of thousands of NSLs will continue to be issued to collect information on innocent Americans because that is exactly what the statute allows.” — American Civil Liberties Union, March 2007

Why is guidance for legal counsel on national security letters needed?

Under federal law, certain federal agencies, such as the Federal Bureau of Investigation (FBI), can request information about individuals in the possession of companies and not-for-profit entities as part of investigations related to national security. The federal government uses national security letters in early stages of national security investigations, and the information gathered under such letters frequently supports the use of other investigative powers, such as those found in the Foreign Intelligence Surveillance Act (FISA), as amended.

Although national security letters have become controversial in debates about the most appropriate ways to balance the protection of national security with respect for civil rights and liberties, the federal government continues to issue national security letters in significant numbers to entities in the United States across the financial, banking, electronic communications, and Internet service provider sectors. Even public libraries...
that provide Internet services to patrons can face the need to respond to a national security letter.\(^6\)

Companies and non-profit entities, and their legal advisors, in these business and service sectors should not wait until the controversies about national security letters settle into equilibrium but should prepare in advance to receive, review, and respond to such letters. The arrival of agents from the FBI at a company’s offices to deliver a national security letter, or a call advising that the FBI is on its way, creates many legal and practical challenges. The effective handling of these challenges connects to issues of security and liberty, potential liability to customers, and possible sanctions against the enterprise imposed by the federal government.

With the stakes so high for recipients of national security letters, the need for legal guidance on receiving, reviewing, and responding to such letters is significant. Recognizing the challenges facing legal counsel to companies across the United States with respect to national security letters, the Cyberspace Law Committee of the American Bar Association (ABA) began this project to produce a practical guide for legal counsel advising companies that may receive and respond to national security letters. The Cyberspace Law Committee collaborated with the Indiana University School of Law—Bloomington and the Center on American and Global Security at Indiana University in crafting this practical Guide.

Members of the ABA Cyberspace Law Committee perceived in important developments increased responsibilities for legal counsel to companies and other entities holding information that might be relevant to national security investigations. The lawsuits filed against telecommunication companies that provided information pursuant to requests from the federal government after September 11, 2001, revealed potential liability problems for companies.\(^7\) Although the federal government did not issue national security letters to these telecommunication companies and later granted such companies retroactive immunity for assisting the government,\(^8\) the controversies and litigation that erupted when the requests and the cooperation of companies became known heightened

\(^6\) Electronic Communications Privacy Act, 18 U.S.C. § 2709(f).
\(^7\) In July 2008, Congress granted the telecommunication companies that cooperated with the federal government after September 11, 2001, retroactive immunity from lawsuits alleging violations of federal privacy statutes. See FISA Amendments Act, supra note 4, at § 201 (instructing federal courts to dismiss civil actions against electronic communication service providers when the Attorney General certifies that such providers assisted the intelligence community pursuant to written requests or directives authorized by the President in the period starting September 11, 2001, through January 17, 2007, with respect to detecting or preventing a terrorist attack against the United States).
\(^8\) Apparently, the federal government issued what are called “exigent letters” to the telecommunication companies, and the statutory law that applies to national security letters does not govern exigent letters. The use of exigent letters by the federal government is controversial, and FBI guidelines on national security letters prohibit the use of exigent letters. See Federal Bureau of Investigation, Comprehensive Guidance on the Use, Requirements, and Reporting of National Security Letters, June 1, 2007, available at http://epic.org/privacy/nsl/New_NSL_Guidelines.pdf (last visited Oct. 4, 2008). Chapter 3 discusses ways to handle receipt of federal government requests for information that do not fall within the statutory law authorizing and regulating national security letters.
concern in the legal community about handling federal government requests for information.

Reports in 2007 and 2008 from the Department of Justice Office of the Inspector General (DOJ/OIG) on the significant increase in the use of national security letters by the FBI underscored these concerns. These reports identified not only mistakes in the FBI’s use of national security letters but also, as discussed more below, errors and problems created by companies that responded to requests for information contained in such letters.

This Guide is not a comprehensive legal hornbook on national security letters, but it contains basic information, analysis, and recommendations that should help inform companies and their legal counsel about the legal and practical challenges of handling national security letters. In order to make the Guide as useful as possible, scholars, experts, and practitioners have reviewed it and provided comments in a cooperative endeavor to develop a resource for legal counsel to companies facing the responsibility of responding to national security letters.

How did the law on national security letters change to produce these challenges for legal counsel?

The nature and seriousness of the challenge national security letters now pose for legal counsel have arisen from the evolution of statutory law in the wake of key judicial and political events. In two seminal decisions in the 1970s, the Supreme Court ruled that the Fourth Amendment did not apply to so-called third-party transactional information held by commercial enterprises, such as banks and telephone companies. These decisions meant the federal government did not need court-approved orders or grand jury subpoenas to access such third-party data during investigations.

Prior to these Supreme Court decisions, Congress had limited the federal government’s ability to obtain information from consumer credit reports in the Fair Credit Reporting Act of 1970. Determined to strengthen privacy protections in response to the Supreme Court decisions, Congress passed two privacy statutes—the Right to Financial Privacy Act of 1978 and the Electronic Communications Privacy Act of 1986—that, among other things, regulated the federal government’s ability to access third-party transactional

---

9 INSPECTOR GENERAL’S 2007 REPORT, supra note 3; INSPECTOR GENERAL’S 2008 REPORT, supra note 1.
11 In producing this Guide, the authors did not solicit any information about specific national security letters. The authors created or derived all examples or hypotheticals in this Guide from publicly available documents or media reports. None of the persons who reviewed drafts of the Guide provided any information concerning any national security letter issued by a U.S. federal government agency. Nothing in this Guide is based on confidential information subject to legal non-disclosure requirements concerning the contents of any national security letter.
12 United States v. Miller, 425 U.S. 435 (1976) (concerning information pertaining to financial services in the hands of financial service providers, such as banks); Smith v. Maryland, 442 U.S. 735 (1979) (concerning information in the hands of telecommunications providers).
information. These statutes created limited exceptions for disclosure of information in connection with national security investigations. Later, in response to concerns about espionage in the United States and terrorism, Congress in the 1990s amended the National Security Act of 1947 and the Fair Credit Reporting Act to allow the federal government to obtain more access through national security letters to transactional information from third-party entities, such as financial institutions and consumer reporting agencies.

Thus, prior to September 11, 2001, Congress had authorized the use of five different kinds of national security letters under four statutes—the National Security Act, the Fair Credit Reporting Act, the Right to Financial Privacy Act, and the Electronic Communications Privacy Act.

Changes to national security letter statutes after September 11, 2001, further broadened the federal government’s ability to obtain transactional information and enhanced the “non-disclosure” or secrecy requirements attached to national security letters. These changes, combined with a significant increase in the number of national security letters issued, transformed a process originally meant to provide some protections for privacy into what many now perceive to be a threat to the Constitution and its protection of Americans’ civil liberties.

In response to judicial decisions holding that the post-September 11 statutes authorizing national security letters violated the First and Fourth Amendments, Congress amended all the national security letter statutes to allow companies that receive national security letters to disclose the receipt of such letters to attorneys for the purpose of obtaining legal advice and assistance. Prior to this change in the law, all the national security letter statutes prohibited the recipient of a national security letter from disclosing it to any person, including outside legal counsel. These 2005 amendments to the non-disclosure requirements have put lawyers for companies at the forefront of effectively responding to national security letters issued by the federal government.

---

Companies and non-profits and their legal counsel confront a complex, confusing, and changing set of rules on national security letters. Multiple statutes authorize the issuance of national security letters by a number of federal agencies. To complicate matters more, the statutes do not use or define key terms in identical ways, which requires close attention to the specific requirements of whatever statute governs any given national security letter. In terms of constitutional law, federal courts are still hearing challenges to the constitutionality of provisions in the national security letter statutes.

What tasks now confront companies and their legal counsel with respect to national security letters?

What is clear amidst the complexity is that legal counsel for recipients of national security letters bear the responsibility for understanding:

- The scope of the relevant statute that authorizes the national security letter in question;
- Whether the requests for information in the national security letter accord with the requirements of the applicable statute;
- Whether the requests for information in the national security letter involve accessing data held outside the United States and thus implicate issues of foreign law on disclosure of personal information or international law on mutual legal assistance; and
- The rights and obligations of the recipient of the national security letter, including, in particular:
  - The presence of any “safe harbors” from liability for disclosing customer information to the federal government;
  - The strict non-disclosure requirements;
  - Procedural obligations towards the federal agency requesting the information; and
  - Rules relating to any legal challenge the recipient might want to mount against the national security letter before a federal court.

---

20 Chapter 2 describes and analyzes this complicated statutory context.
22 Chapter 5 addresses these international issues.
The complexity of the law governing national security letters, and the importance of the national security and privacy objectives in play, make the challenge of responding to national security letters difficult from the perspective of corporate policy and procedures. Companies and their legal counsel have to worry not only about the statutory requirements shaping national security letters but also how the companies organize themselves internally to respond appropriately. For example, companies and their legal counsel must be able to handle many practical challenges in receiving, reviewing, and responding to national security letters, including:

• Handling the initial encounter with the federal agents delivering the national security letter;

• Ensuring that the company complies with non-disclosure requirements applicable to the letter;

• Safeguarding information collected to comply with the letter at all stages of the process;

• Disclosing only the information authorized to be disclosed by the applicable statute and only the information the federal agency requested in the national security letter;

• Keeping adequate records of the company’s response to the letter; and

• Revising corporate policies and procedures that might create difficulties for effectively responding to the letter.

As noted earlier, the DOJ/OIG has identified inappropriate responses from recipients of national security letters as a particular concern. The DOJ/OIG highlighted the over-disclosure of information by recipients of national security letters as a significant problem. In short, recipients of national security letters were providing federal agencies with more information than the agencies requested. Such over-disclosure also played a role in violations of law and policy that DOJ/OIG reported the FBI made in the national security letter process.

As noted above, over-disclosure also may threaten the “safe harbors” the statutes give recipients of national security letters from possible liability to individuals whose information the recipients disclosed to the government. The over-disclosure problem helps illustrate why both the FBI and recipients of national security letters have to improve their policies and procedures with respect to national security letters.

23 INSPECTOR GENERAL’S 2008 REPORT, supra note 1, at 94-100.
How is the Guide organized?

The Guide contains six chapters, and each chapter is organized through a series of questions that raise important issues or features of managing the legal and practical challenges created by receipt of a national security letter. For example, the substantive analysis in Chapter 2 begins with the question: “What is a national security letter?” and Chapter 3 starts with analysis of “What is the likelihood that a company will receive a national security letter?” The Guide does not ask and answer every possible question about handling national security letters, but it focuses on key questions that companies and their attorneys might want answered in preparing to receive, review, and respond to national security letters.

In terms of substantive content, the Guide first provides analysis to help the reader obtain a basic understanding of national security letters (Chapter 2). This chapter explores:

- The basic definition, purpose, and origins of national security letters;
- How national security letters differ from other federal government investigative requests for information (e.g., other administrative subpoenas, court orders, grand jury subpoenas, and FISA orders);
- Why national security letters are controversial;
- What issues of constitutional law national security letters raise;
- The different kinds of national security letters, and which federal agencies can issue them;
- The kind of information federal agencies seek through national security letters; and
- What national security letters look like.

Chapter 3 examines legal and practical tasks that arise when a company receives and reviews a national security letter. The chapter considers the likelihood that a company will receive a national security letter, how a company finds out about a letter issued to it, and what rights and obligations a company has once it has received a letter. The chapter also contains recommendations on what the company and its legal counsel should do in the first encounter with the agents of the federal agency and what information the company should record upon its initial review of the national security letter.

Chapter 4 addresses tasks, issues, and potential problems that companies and their attorneys will encounter in the process of responding to national security letters. The chapter explores the rights and obligations of the company as it responds to national security letters and offers recommendations on ways of making the corporate response process more efficient and effective. The chapter explores other legal and practical issues
companies and their legal counsel may have to think through when responding to a national security letter, such as whether the company should decide not to comply with the letter and challenge it in federal court because the letter does not comply with the authorizing statute.

Chapter 5 focuses on a particular aspect of responding to national security letters—the legal and practical issues that arise if the federal agency seeks information located or held outside the United States by an entity affiliated with the U.S.-based company that received the national security letter. It addresses concerns about the extraterritorial application of federal law and procedures through which the United States seeks information found in other countries, including letters rogatory and Mutual Legal Assistance Treaties (MLATs).

Chapter 6 concludes the Guide’s substantive analysis with thoughts on the need for companies and their legal counsel to monitor continuing developments—politically, legislatively, and judicially—related to national security letters. This chapter examines proposals before Congress that seek to amend the national security letter statutes and offers advice on good sources of information and analysis to consult in staying on the cutting edge of the law and politics of national security letters. It also contains a brief primer on using electronic legal search tools to follow developments in this area.

The Guide also contains a number of appendices that provide material for companies and their legal counsel, including:

- Excerpts from the national security letter statutes (Appendix A);
- Summaries of the leading federal court cases involving litigation on national security letters (Appendix B); and
- Sample company policy covering issues pertaining to receiving, reviewing, and responding to national security letters (Appendix C).

The challenge of balancing security and liberty in the American republic during times of war and danger is difficult and stressful. This Guide focuses on only one aspect of this challenge, but we hope that it helps recipients of national security letters to be able to participate in this balancing task more efficiently. By receiving, reviewing, and responding to national security letters effectively, recipients can uphold the interests and values of their enterprises and the letter and spirit of the rule of law.