

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----  
NICHOLAS MERRILL,

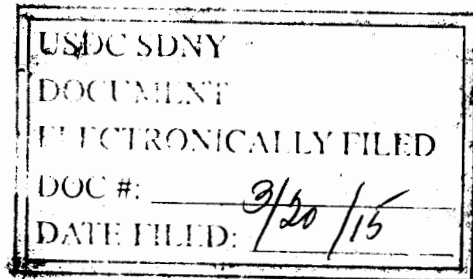
Plaintiff,

v.

No. 14-cv-9763

ERIC HOLDER, Jr., in his official capacity as  
Attorney General of the United States, and  
JAMES B. COMEY, in his official capacity as  
Director of the Federal Bureau of Investigation,

Defendants.  
-----



**UNOPPOSED MOTION OF THE REPORTERS COMMITTEE FOR FREEDOM OF  
THE PRESS AND 21 MEDIA ORGANIZATIONS FOR LEAVE TO FILE  
*AMICI CURIAE* BRIEF IN SUPPORT OF PLAINTIFF**

Michael D. Steger  
STEGER KRANE LLP  
1601 Broadway, 12th Floor  
New York, NY 10019  
(212) 736-6800  
*Counsel of record for amici curiae*

Bruce D. Brown  
Katie Townsend  
Hannah Bloch-Wehba  
REPORTERS COMMITTEE FOR  
FREEDOM OF THE PRESS  
1156 15th Street NW, Ste. 1250  
Washington, D.C. 20005  
(202) 795-9301  
*Of counsel*

The Reporters Committee for Freedom of the Press, American Society of News Editors, Association of Alternative Newsmedia, Association of American Publishers, Inc., Courthouse News Service, Dow Jones & Company, Inc., First Amendment Coalition, Investigative Reporting Workshop at American University, The McClatchy Company, Media Consortium, MediaNews Group, Inc., MPA – The Association of Magazine Media, National Press Photographers Association, Newspaper Association of America, The News Guild - CWA, Online News Association, Radio Television Digital News Association, Reuters America LLC, The Seattle Times Company, Student Press Law Center, Tully Center for Free Speech, and The Washington Post (collectively, “*amici*”), by and through the undersigned counsel, respectfully request permission to file the attached *amici curiae* brief in support of the motion for summary judgment filed by Plaintiff Nicholas Merrill (“Plaintiff”) in the above-captioned action.

All parties consent to the filing of the attached brief.

**IDENTITY OF AMICI**

The Reporters Committee for Freedom of the Press is a voluntary, unincorporated association of reporters and editors that works to defend the First Amendment rights and freedom of information interests of the news media. The Reporters Committee has provided representation, guidance and research in First Amendment and Freedom of Information Act litigation since 1970.

With some 500 members, American Society of News Editors (“ASNE”) is an organization that includes directing editors of daily newspapers throughout the Americas. ASNE changed its name in April 2009 to American Society of News Editors and approved broadening its membership to editors of online news providers and academic leaders. Founded in 1922 as American Society of Newspaper Editors, ASNE is active in a number of areas of interest to top

editors with priorities on improving freedom of information, diversity, readership and the credibility of newspapers.

Association of Alternative Newsmedia (“AAN”) is a not-for-profit trade association for 130 alternative newspapers in North America, including weekly papers like The Village Voice and Washington City Paper. AAN newspapers and their websites provide an editorial alternative to the mainstream press. AAN members have a total weekly circulation of seven million and a reach of over 25 million readers.

Association of American Publishers, Inc. (“AAP”) is the national trade association of the U.S. book publishing industry. AAP’s members include most of the major commercial book publishers in the United States, as well as smaller and nonprofit publishers, university presses and scholarly societies. AAP members publish hardcover and paperback books in every field, educational materials for the elementary, secondary, postsecondary and professional markets, scholarly journals, computer software and electronic products and services. AAP represents an industry whose very existence depends upon the free exercise of rights guaranteed by the First Amendment.

Courthouse News Service is a California-based legal news service for lawyers and the news media that focuses on court coverage throughout the nation, reporting on matters raised in trial courts and courts of appeal up to and including the U.S. Supreme Court.

Dow Jones & Company, Inc., a global provider of news and business information, is the publisher of The Wall Street Journal, Barron’s, MarketWatch, Dow Jones Newswires, and other publications. Dow Jones maintains one of the world’s largest newsgathering operations, with more than 1,800 journalists in nearly fifty countries publishing news in several different languages. Dow Jones also provides information services, including Dow Jones Factiva, Dow

Jones Risk & Compliance, and Dow Jones VentureSource. Dow Jones is a News Corporation company.

First Amendment Coalition is a nonprofit public interest organization dedicated to defending free speech, free press and open government rights in order to make government, at all levels, more accountable to the people. The Coalition's mission assumes that government transparency and an informed electorate are essential to a self-governing democracy. To that end, we resist excessive government secrecy (while recognizing the need to protect legitimate state secrets) and censorship of all kinds.

The Investigative Reporting Workshop, a project of the School of Communication (SOC) at American University, is a nonprofit, professional newsroom. The Workshop publishes in-depth stories at [investigativereportingworkshop.org](http://investigativereportingworkshop.org) about government and corporate accountability, ranging widely from the environment and health to national security and the economy.

The McClatchy Company, through its affiliates, is the third-largest newspaper publisher in the United States with 29 daily newspapers and related websites as well as numerous community newspapers and niche publications.

The Media Consortium is a network of the country's leading, progressive, independent media outlets. Our mission is to amplify independent media's voice, increase our collective clout, leverage our current audience and reach new ones.

MediaNews Group's more than 800 multi-platform products reach 61 million Americans each month across 18 states.

MPA – The Association of Magazine Media, (“MPA”) is the largest industry association for magazine publishers. The MPA, established in 1919, represents over 175 domestic magazine

media companies with more than 900 magazine titles. The MPA represents the interests of weekly, monthly and quarterly publications that produce titles on topics that cover politics, religion, sports, industry, and virtually every other interest, avocation or pastime enjoyed by Americans. The MPA has a long history of advocating on First Amendment issues.

The National Press Photographers Association (“NPPA”) is a 501(c)(6) non-profit organization dedicated to the advancement of visual journalism in its creation, editing and distribution. NPPA’s approximately 7,000 members include television and still photographers, editors, students and representatives of businesses that serve the visual journalism industry. Since its founding in 1946, the NPPA has vigorously promoted the constitutional rights of journalists as well as freedom of the press in all its forms, especially as it relates to visual journalism. The submission of this brief was duly authorized by Mickey H. Osterreicher, its General Counsel.

Newspaper Association of America (“NAA”) is a nonprofit organization representing the interests of more than 2,000 newspapers in the United States and Canada. NAA members account for nearly 90% of the daily newspaper circulation in the United States and a wide range of non-daily newspapers. The Association focuses on the major issues that affect today’s newspaper industry, including protecting the ability of the media to provide the public with news and information on matters of public concern.

The News Guild – CWA is a labor organization representing more than 30,000 employees of newspapers, newsmagazines, news services and related media enterprises. Guild representation comprises, in the main, the advertising, business, circulation, editorial, maintenance and related departments of these media outlets. The News Guild is a sector of the Communications Workers of America. CWA is America’s largest communications and media union, representing over 700,000 men and women in both private and public sectors.

Online News Association (“ONA”) is the world’s largest association of online journalists. ONA’s mission is to inspire innovation and excellence among journalists to better serve the public. ONA’s more than 2,000 members include news writers, producers, designers, editors, bloggers, technologists, photographers, academics, students and others who produce news for the Internet or other digital delivery systems. ONA hosts the annual Online News Association conference and administers the Online Journalism Awards. ONA is dedicated to advancing the interests of digital journalists and the public generally by encouraging editorial integrity and independence, journalistic excellence and freedom of expression and access.

Radio Television Digital News Association (“RTDNA”) is the world’s largest and only professional organization devoted exclusively to electronic journalism. RTDNA is made up of news directors, news associates, educators and students in radio, television, cable and electronic media in more than 30 countries. RTDNA is committed to encouraging excellence in the electronic journalism industry and upholding First Amendment freedoms.

Reuters, the world’s largest international news agency, is a leading provider of real-time multi-media news and information services to newspapers, television and cable networks, radio stations and websites around the world. Through Reuters.com, affiliated websites and multiple online and mobile platforms, more than a billion professionals, news organizations and consumers rely on Reuters every day. Its text newswires provide newsrooms with source material and ready-to-publish news stories in twenty languages and, through Reuters Pictures and Video, global video content and up to 1,600 photographs a day covering international news, sports, entertainment, and business. In addition, Reuters publishes authoritative and unbiased market data and intelligence to business and finance consumers, including investment banking and private equity professionals.

The Seattle Times Company, locally owned since 1896, publishes the daily newspaper *The Seattle Times*, together with *The Issaquah Press*, *Yakima Herald-Republic*, *Walla Walla Union-Bulletin*, *Sammamish Review* and *Newcastle-News*, all in Washington state.

Student Press Law Center (“SPLC”) is a nonprofit, nonpartisan organization which, since 1974, has been the nation’s only legal assistance agency devoted exclusively to educating high school and college journalists about the rights and responsibilities embodied in the First Amendment to the Constitution of the United States. SPLC provides free legal assistance, information and educational materials for student journalists on a variety of legal topics.

The Tully Center for Free Speech began in Fall, 2006, at Syracuse University’s S.I. Newhouse School of Public Communications, one of the nation’s premier schools of mass communications.

WP Company LLC (d/b/a The Washington Post) publishes one of the nation’s most prominent daily newspapers, as well as a website, [www.washingtonpost.com](http://www.washingtonpost.com), that is read by an average of more than 20 million unique visitors per month.

#### **INTEREST OF AMICI**

As members and representatives of the news media, *amici* have a strong interest in ensuring that willing speakers, like Plaintiff, are not restrained from disseminating information of public interest and concern to the press and to the public. The perspective and arguments of *amici* can assist the Court in ruling on Plaintiff’s motion for summary judgment by providing the Court with additional information and analysis not fully addressed by the parties concerning the First Amendment right of the press and the public to receive information from willing speakers, as well as the heightened importance of the public’s receipt of the specific information that Plaintiff seeks to disclose here.

For these reasons, *amici* respectfully request leave to file the attached brief as *amici curiae* in support of Plaintiff's motion for summary judgment.

DATED: March 18, 2015

Respectfully submitted,

/s/ Michael D. Steger

Michael D. Steger (MS 2009)

STEGER KRANE LLP

1601 Broadway, 12th Floor

New York, NY 10019

(212) 736-6800

msteger@skattorney.com

*Counsel of record*

Bruce Brown

Katie Townsend

Hannah Bloch-Wehba

The Reporters Committee for Freedom of the Press

1156 15th St. NW, Suite 1250

Washington, D.C. 20005

(202) 795-9300

*Of counsel*

SO ORDERED. Request GRANTED. The Clerk  
of Court is directed to enter into the  
record of this action the amici curiae  
brief submitted by the organizations  
described above.  
DATE 3-20-15 VICTOR MARRERO, U.S.D.J.



**CERTIFICATE OF SERVICE**

I hereby certify that I electronically filed the foregoing motion and the attached brief of *amici curiae* with the Clerk of the Court for the United States District Court for the Southern District of New York using the CM/ECF system on March 18, 2015.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Dated: March 18, 2015

/s/ Michael D. Steger  
Michael D. Steger

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

NICHOLAS MERRILL,

Plaintiff,

v.

ERIC HOLDER, Jr., in his official capacity as  
Attorney General of the United States, and  
JAMES B. COMEY, in his official capacity as  
Director of the Federal Bureau of Investigation,

Defendants.

14 Civ. 09763 (VM)

~~SEALED~~

STATEMENT OF UNDISPUTED MATERIAL FACTS  
IN SUPPORT OF PLAINTIFF'S MOTION FOR SUMMARY JUDGEMENT

Jonathan Manes  
David A. Schulz  
Benjamin Graham, law student intern  
Nicholas Handler, law student intern  
Matthew Halgren, law student intern  
Amanda Lynch, law student intern  
MEDIA FREEDOM AND INFORMATION  
ACCESS CLINIC  
YALE LAW SCHOOL  
P.O. Box. 208215  
New Haven, CT 06520  
Tel: (203) 432-9387  
Fax: (203) 432-3034  
jonathan.manes@yale.edu

*Counsel for the Plaintiff*

**I. Nicholas Merrill's Role as President of Calyx Internet Access in 2004**

1. Nicholas Merrill is a computer scientist and systems administrator. Merrill Decl. ¶ 2.
2. In 2004, Nicholas Merrill was the president, owner and sole employee of Calyx Internet Access ("Calyx"), a company that, among other things, was an Internet Service Provider ("ISP"). Merrill Decl. ¶ 3.

A. Calyx provided space on the Internet where clients could maintain their own websites and store electronic files. It provided clients with an interface for maintaining their own websites, electronic file storage, email accounts, and sometimes Internet access. Merrill Decl. ¶ 3.

B. Calyx may have collected a wide array of information about its clients, including:

- A client's name, address and telephone number, and other addresses associated with the account;
- Email addresses associated with the account;
- Internet Protocol ("IP") addresses associated with the account;
- Uniform Resource Locator ("URL") addresses assigned to the account;
- Activity logs for the account;
- Logs tracking visitors to the client's website;
- The content of a client's electronic communications;
- Data files residing on Calyx's server;
- The client's customer list;
- The client's bank account and credit card numbers;
- Records relating to merchandise bought and sold; and
- The date the account was opened or closed.

Merrill Decl. ¶ 49.

C. Calyx is now defunct as a corporate entity and is no longer operating. Merrill Decl. ¶ 5.

**II. The National Security Letter and Accompanying Attachment Served Upon Mr. Merrill in 2004**

3. On February 4, 2004, an agent of the FBI served Nicholas Merrill with a National Security Letter ("2004 NSL") demanding that he provide business records containing the "names, addresses, length of service, and electronic communication transactional records" ("ECTR") of a particular client of Calyx (the "Target"). Merrill Decl. ¶¶ 6-7; *id.* Ex. A.
4. Included with the 2004 NSL was a single-page attachment ("Attachment"). Merrill Decl. ¶ 9; *id.* Ex. B.

A. Similar attachments are frequently included with FBI NSLs seeking disclosure of ECTR. Manes Decl. Ex. E, at 5-6.

5. The Attachment provided a non-exhaustive list of specific categories of data that the FBI regarded as ECTR, subject to disclosure in response to the NSL. Merrill Decl. ¶¶ 9, 50; *id.* Ex. B.

A. The categories of data explicitly listed in Attachment were:

- [REDACTED]
- [REDACTED]
- Subscriber name [REDACTED]
- Account number; [REDACTED]
- Address [REDACTED]
- [REDACTED] telephone number [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED] billing [REDACTED]
- [REDACTED]
- [REDACTED] e-mail address [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Merrill Decl. ¶ 50; *id.* Ex. B.

B. Mr. Merrill understood that the NSL sought to impose an obligation on him to turn over any and all categories of records listed in the Attachment pertaining to the Target. Merrill Decl. ¶ 10.

6. Included in the 2004 NSL was a nondisclosure order that forbade Mr. Merrill from revealing that he had received an NSL from the FBI, from revealing the identity of the Target of the NSL, or from revealing anything else about the NSL to any person. Merrill Decl. ¶ 7; *id.* Ex. A.

7. The 2004 NSL certified that the “information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.” Merrill Decl. ¶ 8; *id.* Ex. A.

### III. The Breadth of Organizations and Records Potentially Subject to Compelled Disclosure in Response to a National Security Letter

8. The FBI is authorized by 18 U.S.C. § 2709 to serve an NSL on any “electronic communication service provider.” The term electronic service provider is defined by 18

U.S.C § 2510(15) as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” Many businesses and organizations perform functions that could reasonably be construed as coming within the purview of this statute. These include, among others,

- A. Internet Service Providers. Merrill Decl. ¶ 37.
  - B. Businesses or organizations with a website that enables users to communicate by electronic mail or web forms. Merrill Decl. ¶ 37.
  - C. Search engines such as Google. Merrill Decl. ¶ 38.
  - D. Websites that allow users to post their own content or that allow users to send emails and information requests, such as Amazon or Yelp.com. Merrill Decl. ¶ 38
  - E. Business organizations, non-profit organizations, and educational institutions that provide Internet connectivity to employees, members or students. Merrill Decl. ¶ 39.
9. Businesses, non-profit institutions, and other organizations often maintain a large amount of sensitive information about individuals using their online services, including:
- A. The Internet Protocol (“IP”) addresses assigned to a particular Internet user, records of the electronic communications originating from a specific IP address, and the IP addresses of the recipients of online communications. These records can identify, among other things, the identity of an otherwise anonymous individual communicating on the Internet, the identities of individuals in communication with one another, and the websites (or other Internet content) that an individual has accessed. Merrill Decl. ¶¶ 42–43.
  - B. Records of web transactions by customers, including detailed transaction logs containing the name of every web page accessed, information about the page’s content, the names of accounts accessed, and sometimes username and password combinations. Merrill Decl. ¶ 44.
  - C. “NetFlow” data, which records the transmission of digital information between different online locations. NetFlow data can essentially provide a complete history of each electronic communications service used by a particular Internet user. Merrill Decl. ¶ 45.
  - D. Logs that monitor every email message sent or received on the provider’s servers, or even those that simply pass through its networks. These logs typically include the email headers, including the sender and recipient(s) as well as the subject line. This information can reveal the name of the organization associated with the sender or recipient, the subject matter of the emails, where the message is to be

posted, and any descriptive content included in a user's email address. Merrill Decl. ¶ 46.

E. Logs maintained by web servers containing complete list of all web pages seen by an individual, all search terms, names of email accounts, passwords, purchases made, names of other individuals with whom the user has communicated. Merrill Decl. ¶ 47.

10. Content Delivery Networks such as Akamai and Limelight Networks, which are high-availability networks used by certain highly trafficked websites, record every image, webpage, video clip, or other "object" downloaded by every user of their client websites. These networks can serve as independent sources of a user's web browsing history through the records that they store. Merrill Decl. ¶ 48.

#### **IV. Sensitive Personal Information That May Be Revealed by Disclosure of the Types of Records Listed in the Attachment**

11. The types of records listed in the Attachment can disclose highly sensitive details about an individual's life. Merrill Decl. ¶ 51.

12. Sensitive information that might be derived about an individual from analyzing the types of records described in the 2004 Attachment include:

A. Details about a person's intimate relationships, religious, political and community affiliations, intellectual pursuits, political leanings, long-term plans, financial condition, and medical concerns. Merrill Decl. ¶ 51.

B. Sensitive organizational or professional associations, or otherwise confidential associations—for example, between a user and Alcoholics Anonymous, a lawyer, a psychiatrist, or a newspaper tip line. Merrill Decl. ¶ 52.

C. The identity of individuals engaging in anonymous online speech. Merrill Decl. ¶ 53.

D. The identity of individuals involved in religious or political associations. Merrill Decl. ¶ 53.

E. Information that may emerge from computer-aided analysis of entire sets of data, producing detailed insight regarding individuals and associations. For instance, datasets like those that NSLs would generate may be used to produce social graphs mapping out the individuals and organizations with whom an individual has communicated, and predictive models allow analysts to use known patterns of activity to predict certain attributes of individuals and organizations, like race, religion, leadership structure, or strength of certain personal and professional relationships. Merrill Decl. ¶ 54.

**V. Previous Litigation Challenging the 2004 NSL and Non-Disclosure Order**

13. In April of 2004, Mr. Merrill, along with Calyx and the American Civil Liberties Union (“ACLU”), filed suit to challenge the constitutionality of both the NSL’s nondisclosure requirement and its demand that he disclose the information sought in the 2004 NSL and Attachment. Nicholas Merrill was identified as “John Doe” in the lawsuit, and Calyx Internet Access was identified as “John Doe, Inc.” Merrill Decl. ¶ 11.
14. After more than five years of litigation, including two appeals to the Court of Appeals for the Second Circuit, the Southern District of New York sustained the nondisclosure order against Mr. Merrill in October 2009. Merrill Decl. ¶¶ 11-17.
15. After Mr. Merrill filed a Motion to Reconsider, the District Court issued an order requiring that the government publicly release a less redacted version of the Attachment that included “(1) material within the scope of information that the NSL statute identifies as permissible for the FBI to obtain through use of NSLs, and (2) material that the FBI has publicly acknowledged it has previously requested by means of NSLs.” *Doe v. Holder*, 703 F. Supp. 2d 313, 316 (S.D.N.Y. 2010); Merrill Decl. ¶ 18; *id.* Ex. C.
16. Following the ruling, while that decision was pending on appeal, the parties reached a settlement in 2010 permitting Mr. Merrill to identify himself as the plaintiff and recipient of the NSL at issue in the litigation. Merrill Decl. ¶ 19.
17. Mr. Merrill has since publicly identified himself as the recipient of the NSL at issue in the *Doe* litigation and as the plaintiff in prior litigation challenging the NSL’s legality. Merrill Decl. ¶ 20.

**VI. Current Scope of the Nondisclosure Order**

18. Between 2010 and 2014, Mr. Merrill was not contacted by the government regarding the scope of the remainder of the nondisclosure order. Merrill Decl. ¶ 21.
19. In January 2014, Mr. Merrill, through *pro bono* counsel, contacted the government’s counsel to inform the government that he intended to sue to challenge the legality of the remaining nondisclosure order, and to request that the agency lift the remainder of the nondisclosure order voluntarily. Merrill Decl. ¶ 23; Manes Decl. ¶ 3, 5.
20. In February 2014, the FBI communicated, through counsel, that it did not intend to lift the nondisclosure order as it pertained to the non-public portions of the Attachment, but that it would agree to lift the rest of the nondisclosure order. Manes Decl. ¶ 6. Merrill Decl. ¶ 23.
21. The FBI’s agreement to partially lift the nondisclosure order was embodied in a Stipulation and Order entered by the Court on April 15, 2014. Manes Decl. ¶¶ 2, 8; *id.* Ex. A.

22. Mr. Merrill remains forbidden from speaking about the contents of the Attachment, except to the extent specified in the Court's decision in *Doe v. Holder*, 703 F. Supp. 2d 313, 316 (S.D.N.Y. 2010). Manes Decl. ¶ 2; *id.* Ex. A.
23. Aside from disclosing the contents of the Attachment, Mr. Merrill may speak publicly about anything relating to the 2004 NSL, including publicly disclosing the Target of the 2004 NSL, discussing the 2004 NSL with its target, and speaking about all other circumstances surrounding issuance of the NSL or the ensuing litigation. Manes Decl. Ex. A.
24. Following entry of the April 15, 2014, Stipulation and Order, Mr. Merrill communicated to the Target that he or she had been the subject of an NSL issued by the FBI seeking disclosure of information about him or her. Merrill Decl. ¶ 24.
25. The investigation of which the 2004 NSL was part is now closed. Manes Decl. ¶¶ 6-7, 10; *id.* Ex. A.
26. The government intends the current nondisclosure order to remain in effect permanently or indefinitely. Manes Decl. ¶¶ 6-7, 10; *id.* Ex. A; Merrill Decl. ¶ 33.
27. The duration of the current nondisclosure order is untethered from any considerations specific to the investigation that prompted the 2004 NSL. Manes Decl. ¶¶ 6-7, 10; *id.* Ex. A; Merrill Decl. ¶ 33.
28. In the event that the current legal challenge to the nondisclosure order fails, the government will not, of its own accord, undertake to review the continuing necessity of the nondisclosure order, nor will it notify Mr. Merrill if it believes the nondisclosure order is no longer required. Merrill Decl. ¶¶ 21, 32-33; Manes Decl. ¶¶ 6-7, 10; *id.* Ex. A.

**VII. The Widespread Issuance of NSLs and the Extent of Disclosure Regarding the Scope of the FBI's Claimed NSL Authority**

29. The FBI has issued tens of thousands of NSLs each year to Internet Service Providers and other entities deemed "electronic service providers." It has issued hundreds of thousands of NSLs since 2001. Manes Decl. ¶ 12.
  - A. None of the recipients of these NSLs has publicly disclosed the categories of "electronic communications transactional records" requested by the FBI. Merrill Decl. ¶ 27; Manes Decl. ¶ 16.
  - B. The categories of data and records that the FBI believed that it could compel from ISPs in 2004 are not publicly defined in any statute, regulation, administrative guidance, judicial decision, or other public document. Manes Decl. ¶ 16.
  - C. The categories of data and records that the FBI believes it is currently authorized to compel from ISPs are also not publicly defined in any statute, regulation,



administrative guidance, judicial decision, or other public document. Manes Decl. ¶ 16.

D. Tens of thousands of NSLs issued by the FBI seek disclosure of information about U.S. citizens and other U.S. persons. Manes Decl. ¶ 14.

30. In 2008, the Department of Justice's Office of Legal Counsel issued a memorandum in response to queries from the FBI regarding the scope of its NSL authority. The memorandum indicated that the FBI's authority to obtain ECTR "reaches only those categories of information parallel to subscriber information and toll billing records for ordinary telephone service." Manes Decl. ¶ 15; *id.* Ex. I.

A. Neither the OLC's memorandum, nor any subsequent statute, regulation, administrative guidance or judicial opinion clarifies what types of records are the electronic "parallel" of traditional subscriber information and toll billing records. Manes Decl. ¶ 15-16; *id.* Ex. I.

B. The FBI has not published any regulations, guidance, or other statements indicating whether the 2008 memorandum resulted in a substantive change in its understanding of the scope of its NSL authority. Manes Decl. ¶ 16.

31. The government has publicly acknowledged that it uses NSLs to collect some of the categories of data that are listed in the Attachment and currently subject to the non-disclosure order. For example:

A. A December 23, 2002, letter from the Department of Justice to Senator Leahy that was published in a Senate Report acknowledged that the FBI used NSLs to collect

[REDACTED]

[REDACTED] all of which appear in the Attachment but remain subject to the nondisclosure order. Manes Decl. Ex. J.

B. A March 2007 report by the Department of Justice's Office of the Inspector General acknowledged that the FBI uses NSLs to collect "email [REDACTED] [REDACTED] both of which are redacted or partially redacted from the public version of the Attachment under the current nondisclosure order. The March 2007 Report also states that NSLs may be used to obtain "billing records and methods of payment," types of information that appear to be encompassed by categories that remain suppressed in the Attachment. Manes Decl. Ex. K.

32. A manual published by the DOJ's Office of Legal Education provides a sample attachment that may be appended to a disclosure order issued pursuant to 18 U.S.C. § 2703, listing the categories of records sought pursuant to such an order. That attachment lists categories of records that are very similar to those listed in the Attachment to the 2004 NSL. Manes Decl. Ex. L.

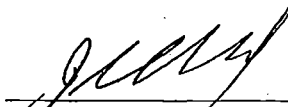
### VIII. Public Controversy and Political Debate Regarding NSLs

33. NSLs have been the subjects of public controversy for over a decade. Manes Decl. ¶ 20.
34. The FBI has in the past extensively misused its NSL authority. Manes Decl. ¶¶ 23-24; *id.* Exs. K, Q.
35. Following a series of unauthorized disclosures in 2013 regarding the government's bulk collection of domestic telephone records and other surveillance programs, there has been an intense public and legislative debate regarding the permissible scope of the government's surveillance authorities. Manes Decl. ¶¶ 24-25, 27; *id.* Exs. Q, S; H.R. 3361, 113th Cong. (2013); S. 2685, 113th Cong. (2014).
  - A. For instance, there was widespread concern when the public learned that the FBI had persuaded the Foreign Intelligence Surveillance Court to allow bulk collection of all domestic calling records on the theory that all such "business records" were "relevant" to a counterterrorism investigation and therefore subject to disclosure under Section 215 of the USA PATRIOT Act, 50 U.S.C. § 1861. Manes Decl. ¶ 24; *Klayman v. Obama*, 957 F. Supp. 1 (D.D.C. 2013).
36. The scope of the government's NSL authority has come under significant scrutiny from members of the public, experts, and official bodies since 2013. Manes Decl. ¶¶ 23-27.
37. There have been serious efforts to propose reforms to the NSL statute since 2013. Manes Decl. Ex. Q; 160 Cong. Rec. H4803 (daily ed. May 22, 2014) (USA FREEDOM Act H.R. 3361, 113th Cong. (2013), passes House by a vote of 303-121); 160 Cong. Rec. S6079 (daily ed. Nov. 18, 2014) (USA FREEDOM Act, S. 2685, 113th Cong. (2014), receives 58 votes in Senate on cloture motion).
38. The President's Review Group on Intelligence and Communications Technologies recommended that NSL nondisclosure orders be subject to initial judicial authorization and frequent automatic judicial review. It also recommended that all NSL recipients be permitted to disclose the categories of information produced in response to FBI demands. Manes Decl. ¶ 26, *id.* Ex. Q.
39. President Obama has stated that the government can and should be more transparent about how the government uses national security letters and has directed the Attorney General to amend how the government uses national security letters so that secrecy will not be indefinite. Manes Decl. ¶ 28; *id.* Ex. S.
40. The FBI has adopted a policy of presumptively terminating NSL nondisclosure orders at the earlier of three years after the opening of a fully predicated investigation or the investigation's close, and that continuing nondisclosure obligations should be imposed only on a case-by-case basis. Manes Decl. ¶ 29; *id.* Ex. T.

**IX. Mr. Merrill's Advocacy on Issues of Privacy and Government Surveillance, and Desire to Educate the Public Regarding the Scope of the FBI's Claimed NSL Authority**

41. Mr. Merrill is the Executive Director and Founder of the Calyx Institute, a non-profit education and research organization devoted to studying, testing, developing, and implementing "privacy by design" through functional privacy and anonymity controls. The Institute pursues these aims as part of its mission of promoting free speech, civic engagement, and privacy rights online and in the mobile technology industry. Merrill Decl. ¶ 1.
42. Mr. Merrill has actively contributed to public debates regarding the FBI's use and abuse of NSLs and other issues relating to government surveillance and secrecy, as well as citizens' rights to privacy in records of their online communications and other activities. Merrill Decl. ¶¶ 1-2, 28-31, 34, 56; Manes Decl. ¶¶ 21-22; *id.* Exs. N, O, P.
  - A. Mr. Merrill has received awards and other significant public recognition for his advocacy relating to National Security Letters. Manes Decl. ¶¶ 21-22, Exs. N, O, P.
43. In 2007, while still forbidden from revealing his identity as an NSL recipient, Nicholas Merrill anonymously published an opinion editorial for the *Washington Post* newspaper detailing his experience receiving an NSL from the FBI in 2004. Merrill Decl. ¶ 28.
44. Mr. Merrill believes that the public would be alarmed by the range of information the FBI collects about private citizens through the use of NSLs, were such information made public. Merrill Decl. ¶ 31.
45. Mr. Merrill would inform the public regarding the scope of the FBI's claimed surveillance authority as specified in the Attachment, but is prevented from doing so by the current nondisclosure order. Merrill Decl. ¶ 31.
46. Mr. Merrill wishes to explain to the public why various categories of records listed in the Attachment implicate significant concerns regarding individual privacy, freedom of speech, and freedom of association, but is prevented from doing so by the current nondisclosure order. Merrill Decl. ¶ 31.
47. Mr. Merrill wishes to advocate for legislative changes to the NSL statute that would clarify and narrow the scope of the FBI's NSL authority, but is prevented from effectively doing so by the current nondisclosure order. Merrill Decl. ¶ 31.
48. Mr. Merrill has been prevented from engaging in a range of speech and advocacy relating to the scope of the FBI's use of NSLs by virtue of the continuing nondisclosure order. Merrill Decl. ¶¶ 28, 31, 34, 56.

Respectfully submitted,



---

Jonathan Manes, supervising attorney  
David A. Schulz, supervising attorney  
Benjamin Graham, law student intern  
Nicholas Handler, law student intern  
Matthew Halgren, law student intern  
Amanda Lynch, law student intern  
MEDIA FREEDOM AND INFORMATION  
ACCESS CLINIC  
YALE LAW SCHOOL  
P.O. Box. 208215  
New Haven, CT 06520  
Tel: (203) 432-9387  
Fax: (203) 432-3034  
jonathan.manes@yale.edu

*Counsel for the Plaintiff*

Dated: New Haven, CT  
March 10, 2015

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

NICHOLAS MERRILL,

Plaintiff,

v.

ERIC HOLDER, Jr., in his official capacity as  
Attorney General of the United States, and  
JAMES B. COMEY, in his official capacity as  
Director of the Federal Bureau of Investigation,

Defendants.

14 CIV. 09763 (VM)

**SEALED**

DECLARATION OF NICHOLAS MERRILL

I, Nicholas Merrill, hereby declare:

1. I am the Executive Director and Founder of the Calyx Institute, a non-profit education and research organization devoted to studying, testing, developing, and implementing “privacy by design” through functional privacy and anonymity controls. The Institute pursues these aims as part of its mission of promoting free speech, civic engagement, and privacy rights online and in the mobile technology industry.

2. I am a computer scientist and systems administrator dedicated to building experimental privacy-protective options for Internet users, including developing a ubiquitously encrypted public test bed and convenient security software models for public use and education. At the Calyx Institute, for example, I operate an optimally secure experimental free public conferencing service and I am currently working to build an encrypted Internet Exchange called CRYPTO-IX, among other projects. Through the Calyx Institute, I have also launched Canary Watch with several partners to monitor when organizations that post “warrant canaries”—

regularly published statements announcing that the organization has not received a demand from the government to produce information about its users—have altered or taken down those statements.

3. In February 2004, I was the president, owner, and sole employee of Calyx Internet Access, an Internet access and consulting business that was incorporated and located in Manhattan, New York. Calyx Internet Access provided clients with an interface for maintaining their own websites, electronic file storage, email accounts, and sometimes Internet access.

4. Calyx Internet Access had both paying and non-paying clients, some of whom engaged in controversial political speech. Some of our clients communicated anonymously or pseudonymously, allowing them to discuss sensitive or controversial subjects without fear of retaliation or reprisal.

5. I ceased operating Calyx Internet Access in August 2004, and the company is now defunct.

*The National Security Letter*

6. More than a decade ago, I received a National Security Letter (“NSL”) from the FBI. On or about February 4, 2004, an FBI agent served the offices of Calyx Internet Access in Manhattan with a copy of the NSL. Attached as Exhibit A is a true and correct copy of the first two pages of the letter I received in 2004, as previously redacted.

7. The NSL ordered that I “provide the [FBI] the names, addresses, lengths of service and electronic communication transactional records” pertaining to one of Calyx’s clients. The letter stated that I was not allowed to tell anyone, including my client, that the FBI was seeking information through an NSL. The letter prohibited me, or my agents or employees, “from disclosing to any person that the FBI has sought or obtained access to information or records

under these provisions,” pursuant to 18 U.S.C. § 2709(c). It also required that I provide responsive records personally to an FBI representative. The letter did not permit me to “send the records through the mail nor disclose the substance of [the] request in any telephone conversation.”

8. The NSL included a certification that “the information sought [was] relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.”

9. The NSL included an Attachment, which identified specific client records demanded by the FBI and elaborated upon what types of records count as “electronic communication transactional records.” Attached as Exhibit B is a true and correct copy of the unredacted Attachment.

10. I understood that the NSL sought to require me to turn over any types of data listed in the NSL, including any and all types of records listed in the Attachment.

### ***Previous Litigation***

11. After receiving the NSL, I sought and obtained legal advice and representation from lawyers at the American Civil Liberties Union. On April 6, 2004, I initiated a lawsuit challenging the constitutionality of the NSL statute, both with regard to the FBI’s authority to force me to turn over the information sought in the NSL and Attachment as well as the gag order that accompanied the NSL. Because I was forbidden from disclosing the fact that I had received the NSL, I was identified in the lawsuit as “John Doe.” Calyx Internet Access (identified as “John Doe, Inc.”), the American Civil Liberties Union (“ACLU”) and the American Civil Liberties Union Foundation (“ACLUF”) were co-plaintiffs in the case, which was filed in the U.S. District Court for the Southern District of New York, Case No. 04 Civ. 2614 (VM).

12. On September 28, 2004, the District Court issued an opinion striking down the NSL statute, 18 U.S.C. § 2709, because it violated the First Amendment to the U.S. Constitution. The Court's opinion also found that the NSL that had been issued to me violated the Fourth Amendment to the U.S. Constitution. The Court's decision is reported as *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

13. The government appealed the District Court's decision. While that appeal was pending, and largely in response to the victory in District Court, Congress amended the NSL statute. In a decision dated May 23, 2006, the Court of Appeals for the Second Circuit remanded the case to the District Court so that the District Court could, in the first instance, address the constitutional infirmities of the law, as revised by Congress. The Court of Appeals' decision is reported as *Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006).

14. After my case was remanded to the District Court, the government filed a declaration dated November 7, 2006, indicating that the FBI was no longer demanding that I comply with the 2004 NSL. Even though the government was no longer seeking to force me to disclose records about my client, it nevertheless continued to enforce and defend a total gag order forbidding me from even identifying myself as a plaintiff in the ongoing litigation.

15. In a decision dated September 6, 2007, the District Court again struck down the NSL statute and invalidated the gag order imposed upon me. This decision is reported as *Doe v. Gonzales*, 500 F. Supp. 2d 397 (S.D.N.Y. 2007).

16. The government again appealed the District Court's decision. The Court of Appeals, like the District Court, determined that the NSL statute did not comply with the First Amendment, but it ruled on narrower grounds and issued a narrower remedy, declining to strike the statute down in its entirety. For a second time, the Court of Appeals remanded the case to the



District Court, this time in order to give the government an opportunity to attempt to justify the continuing gag order on me under the newly articulated standards. This decision is reported as *John Doe, Inc. v. Mukasey*, 549 F.3d 861 (2d Cir. 2008).

17. On remand, in a decision dated October 20, 2009, the District Court initially held that the government had met its burden to justify the gag order in its entirety, while emphasizing that the gag did not then constitute a permanent ban on speech. That decision is reported as *Doe v. Holder*, 665 F. Supp. 2d 426 (S.D.N.Y. 2009).

18. On March 18, 2010, in response to a motion for reconsideration filed on behalf of me and my co-plaintiffs, the District Court ordered the government to lift the nondisclosure requirement with respect to certain limited portions of the Attachment listing categories of records that were either mirrored in the NSL statute itself or that the FBI had publicly acknowledged it had previously requested using NSLs. The gag order otherwise remained fully in place. That decision is reported as *Doe v. Holder*, 703 F. Supp. 2d 313 (S.D.N.Y. 2010). A true and correct copy of the redacted Attachment, as made public disclosed following this 2010 decision, is attached as Exhibit C.

19. Along with my co-plaintiffs, I appealed the District Court's decision. While that appeal was pending, I reached a settlement agreement with the FBI. Under that agreement, I was finally allowed to identify myself as the recipient of the 2004 NSL and as the plaintiff in the lawsuit. That settlement was memorialized in a Stipulation and Order of Dismissal filed in the District Court on July 30, 2010.

20. As a result of that settlement, I finally identified myself as the recipient of the NSL at issue after more than six years subject to a complete and debilitating gag order. During those six years, I had been forced to lie to those close to me and many others with whom I interacted in

order to conceal meetings with my attorneys and other activities related to the lawsuit, lest I reveal that I was the “John Doe” plaintiff in the case. This was particularly difficult because the case was often the subject of intense media interest and was extensively discussed among my colleagues in the computer security and privacy field. As a result, I was forced to constantly censor myself, and was almost entirely unable to engage in public advocacy on the issue of NSLs, for fear of violating the gag order imposed on me.

***Current Scope of the Gag Order***

21. Between the 2010 settlement and 2014, the government never contacted me to assert the continuing necessity of the gag order. To my knowledge, the government also did not contact the Court or any of my attorneys.

22. During this time, I had to continue to carefully censor myself, even though I could identify myself as the recipient of the 2004 NSL and the plaintiff in the long-running litigation. This continued to hamper my ability to participate in public debate and discussion regarding NSLs, and it continued to affect my interactions with relatives, friends, and colleagues.

23. In April 2014, I notified the FBI, through *pro bono* counsel at the Media Freedom and Information Access Clinic at Yale Law School, that I intended once again to challenge the continuing gag order. Given how much time had passed since the NSL was issued, I asked the FBI to voluntarily drop the gag order in its entirety. In response, the government refused to lift the gag order with respect to the contents of the Attachment to the 2004 NSL (except to the extent the District Court had lifted small portions of that gag in its March 2010 decision, described above). The government, however, agreed to lift the gag order in all other respects, citing “changed circumstances.” As a result, I was permitted, for example, to disclose the target

of the 2004 NSL, and to discuss the 2004 NSL with its target. But I am still unable to speak about nearly everything included in the 2004 Attachment.

24. After the relevant portion of the gag was lifted, I communicated to the target of the NSL that the FBI had requested information about him or her.

25. It is my understanding that the investigation of which the 2004 NSL was part has now concluded. This understanding is based, among other things, on the fact that I have been permitted by the FBI to discuss the 2004 NSL with its target.

26. I understand from official government reports, news coverage, and other sources that many tens of thousands of NSLs have been issued since 2001.

27. To my knowledge, no other NSL recipient has been permitted to publicly reveal the target of an NSL issued to him or her, or to discuss an NSL with its target. To my knowledge, I am the only NSL recipient who remains subject to an NSL gag order that is limited solely to the contents of the Attachment – *i.e.*, a gag order that only forbids discussion of the *types* of records sought in an NSL, while permitting unfettered discussion of any and all other circumstances relating to the issuance of the NSL, its target, and the particular investigation that prompted it. To my knowledge no NSL recipient has yet been permitted to disclose the full contents of the Attachment or to discuss the FBI's understanding of the scope of its authority to compel disclosure of "electronic communication transactional records" ("ECTR").

***Interference with Public Participation and Advocacy***

28. Since I first received the NSL in 2004, I have been strongly committed to engaging in public advocacy regarding the FBI's use and abuse of NSLs. Even while I was subject to a complete gag order prior to the 2010 settlement, I sought to engage in the public and legislative

debate regarding NSLs by publishing an anonymous op-ed in the *Washington Post* in 2007. But the gag order consistently and significantly constrained my efforts at public advocacy.

29. Even now, more than a decade later, I cannot speak about the contents of the 2004 Attachment.

30. The Attachment identifies the categories of records the FBI ordered me to produce and reveals what the FBI considers to be ECTR under the NSL statute.

31. I believe that the public would be alarmed if they knew what kinds of records the FBI apparently believes constitute ECTR and can therefore obtain simply by issuing an NSL, without any prior judicial review or any meaningful likelihood of judicial oversight. I would like to explain to the public why various categories of records listed in the Attachment implicate significant concerns in terms of individual privacy, freedom of speech, and freedom of association. I would also like to be able to advocate for legislative changes to the NSL statute that would clarify and rein in the FBI's authority. But because I remain gagged with respect to the Attachment, I am unable to engage in such public education and advocacy. In fact, because of the remaining gag order, I must vigilantly censor myself when discussing the FBI's abuses and potential abuses of NSLs. The current nondisclosure order therefore continues to restrict my ability to speak out on important matters of public concern about which I would otherwise speak.

32. The government has not indicated that it will ever undertake to review the continuing necessity of the gag order, absent the threat of another legal challenge. I have no reason to believe that the government will contact me if ever the government were to decide that the gag is no longer necessary. Indeed, if I had not found and engaged *pro bono* counsel to threaten the present litigation, I would remain subject to the 2010 gag order, even though the FBI readily

conceded (in response to the threat of litigation) that “changed circumstances” had rendered most of the gag order unnecessary.

33. Therefore, if the gag order is not lifted in its entirety during the course of this litigation, I will remain subject to a gag order permanently. It is my understanding that the gag order has now become untethered from any circumstances specific to the 2004 NSL, or the investigation of which it was part, and that the government intends to permanently forbid me from discussing the contents of the Attachment.

34. Given my personal and professional commitment to discussing online privacy and government surveillance policy, the government’s permanent gag on my speech continues to significantly hamper my ability to engage in the public debates in which I am most professionally and personally invested.

***The Scope of Information Subject to Disclosure via NSLs***

35. NSLs implicate serious privacy, free speech, and freedom of association concerns because of (i) the wide variety of electronic service providers potentially subject to NSLs, (ii) the vast amount of potentially sensitive information that such electronic service providers maintain about their clients, and (iii) the FBI’s expansive understanding of the types of records that count as ECTR and are subject to compelled disclosure in response to an NSL.

36. These concerns are particularly acute because NSLs may be issued without any prior judicial oversight, and without any real prospect of judicial review after their issuance. To my knowledge, only a handful of the more than tens of thousands of NSLs issued by the FBI since 2001 have been challenged in court. I am aware of no court decision that has ever determined the lawful scope of the FBI’s authority to compel production of records using NSLs, including whether its understanding of what constitutes ECTR complies with the NSL statute or with the

Constitution. In my case, the government mooted my ability to challenge the lawfulness of the FBI's claimed NSL authority when it indicated in 2006 that the FBI was no longer demanding that I comply with the NSL.

***Businesses and Other Organizations Subject to NSLs***

37. A potentially vast array of businesses and organizations are potentially subject to NSLs. According to the NSL statute, 18 U.S.C. § 2709, any "electronic communication service provider" may be served with an NSL demanding disclosure of records. Given the expansive meaning of electronic communications service, defined in 18 U.S.C § 2510(15) as "any service which provides to users thereof the ability to send or receive wire or electronic communications," it is my belief and understanding that the term applies to an extremely broad range of businesses and organizations. It clearly applies to Internet Service Providers, like Calyx Internet Access as it existed in 2004. However, the statute also appears to cover any business or organization with a website that enables users to communicate through email or web forms. For example, the Calyx Institute's website, which includes sign-up and contact forms for interested users, may well qualify.

38. The statute also clearly covers search engines like Google. To use a search engine, users enter requests and send them to the search engine, which performs the requested search and then transmits back the results. All websites that allow users to post their own content or that enable users to send emails and information requests also likely fall under the statute. Websites like Amazon or Yelp.com would therefore also appear to qualify as electronic communication service providers.

39. Most businesses and organizations, as well as schools and universities, provide Internet connectivity to their employees or students so that they can communicate. Each of these entities is therefore also likely to be considered a service provider under the statute.

***Sensitive Information Typically Maintained by Organizations Subject to NSLs***

40. Businesses and other organizations subject to NSLs will often maintain a large amount of sensitive information about individuals using their online services.

41. Based on my extensive experience working as an ISP operator, systems administrator, and experimental software designer since 1995, and based on my extensive collaborations with other computer scientists, computer engineers, and information technology professionals, I have a detailed understanding of the kinds of records that electronic communication service providers can and do typically maintain.

42. Each device participating in a specific network is assigned a unique, 32-bit numerical label, which is that computer's Internet Protocol ("IP") address. In order to send information over the Internet, the information must first be separated into small "packets," each of which consists of a header and a data payload. The header includes the originating IP address, the destination IP address, a number defining the IP protocol in use, and other information used to interpret the data payload.

43. Electronic communication service providers can maintain records of the IP addresses assigned to particular individuals and of the electronic communications involving that IP address. These records can identify, among other things, the identity of an otherwise anonymous individual communicating on the Internet, the identities of individuals in communication with one another, and the websites (or other Internet content) that an individual has accessed.

44. Electronic communication service providers can also monitor and store information regarding web transactions by their users. These transaction logs can be very detailed, including the name of every web page accessed, information about the page's content, the names of accounts accessed, and sometimes username and password combinations. This monitoring can occur by routing all of a user's traffic through a proxy server or by using a network monitoring system.

45. Electronic communication service providers can also record Internet "NetFlow" data. This data consists of a set of packets that travel between two points. Routers can be set to automatically record a list of all the NetFlows that they see, or all the NetFlows to or from a specific IP address. This NetFlow data can essentially provide a complete history of each electronic communications service used by a particular Internet user.

46. Electronic communication service providers that provide email services also maintain "log" files that monitor every email message sent or received on the provider's servers. These logs typically include the email headers, including the sender and recipient(s) as well as the subject line. This information can reveal the name of the organization associated with the sender or recipient, the subject matter of the emails, where the message is to be posted, and any descriptive content included in a user's email address. Many communication service providers also use network monitoring systems to create log files for messages that merely pass through their networks.

47. Web servers also often maintain logs of every request that they receive and every web page that is served. This could include a complete list of all web pages seen by an individual, all search terms, names of email accounts, passwords, purchases made, names of other individuals with whom the user has communicated, and so on.



48. Content Delivery Networks, such as Akamai and Limelight Networks, are high-availability networks that popular websites use to increase the speed at which their content is delivered to users. For example, many of the country's top media, entertainment, and electronic commerce companies use Akamai's services to store images and other rich content so that users can download their pages more quickly. These Content Delivery Networks record every image, webpage, video clip, or other "object" downloaded by every user of their client websites. Content Delivery Networks can therefore serve as independent sources of a user's web browsing history through the records that they store.

49. Calyx Internet Access, like most ISPs, collected a wide array of information about its clients. For a given client, we may have collected their name, address and telephone number; other addresses associated with the account; email addresses associated with the account; IP addresses associated with the account; Uniform Resource Locator (URL) addresses assigned to the account; activity logs for the account; logs tracking visitors to the client's website; the content of a client's electronic communications; data files residing on Calyx's server; the client's customer list; the client's bank account and credit card numbers; records relating to merchandise bought and sold; and the date the account was opened or closed.

***Records Regarded by the FBI as ECTR Can Reveal Sensitive Personal Information***

50. The Attachment to the NSL that the FBI served me with listed various categories of records constituting ECTR that the FBI sought to obtain. These categories of records constituting ECTR included:

- [REDACTED]
- [REDACTED]
- Subscriber name [REDACTED]
- [REDACTED]
- Address [REDACTED]
- [REDACTED] telephone numbers

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED] billing [REDACTED]
- [REDACTED]
- [REDACTED] e-mail address [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

51. Even though the types of information collected by NSLs have been characterized as “non-content” data, they can nonetheless reveal extremely sensitive, substantive and personal information. Even a cursory analysis of electronic communications transactional records—such as [REDACTED]—can reveal a person’s intimate relationships, religious, political and community affiliations, intellectual pursuits, political leanings, long-term plans, financial condition, medical concerns, and more.

52. It is often trivially easy to connect a single data point to an identity. Particular email addresses, telephone numbers, or [REDACTED] can be matched with organizations whose identity is inherently revealing—for example, Alcoholics Anonymous, a lawyer, a psychiatrist, or a newspaper tip line.

53. Even merely identifying the name of a client associated with a particular [REDACTED] can reveal sensitive information. Such disclosure can serve to unmask an individual engaging in protected anonymous speech online. It can also reveal the identities of individuals involved in religious or political associations.

54. Because “non-content” data is constantly generated, is often highly structured, and can therefore be more easily analyzed, the informational yields can be much higher. It is easy to draw inferences from patterns of communication using non-content information. Publicly available software packages like MIT’s Immersion permit users to generate social graphs from

datasets like those that NSLs could be used generate. These graphs map out the individuals and organizations with whom an individual has communicated. Predictive models allow analysts to use known patterns of activity to predict certain attributes of individuals and organizations, like race, religion, leadership structure, or strength of certain personal and professional relationships.

55. In short, understanding which types of records the FBI believes it is authorized to obtain from electronic communication service providers by merely issuing an NSL is critical to assessing the substantial privacy interests at stake.

56. The Attachment to the 2004 NSL describes many of the types of records that the FBI evidently believes it can obtain using an NSL. Because I am forbidden from discussing the contents of the Attachment, I am unable to explain the significant privacy concerns implicated by the FBI's expansive use of NSLs and to alert the public to the significant potential for abuse. For the same reason, I am unable to contribute to recurrent debates in Congress over the legitimate scope of—and necessary checks on—the government's surveillance powers under the NSL statute and other provisions of the USA PATRIOT Act and other laws.

I declare under penalty of perjury that the foregoing is true and correct. Executed on March 9, 2015 at New York, NY.

*Nicholas Merrill*

---

Nicholas Merrill

# **EXHIBIT A**



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

[REDACTED] 2004

[REDACTED]  
President  
[REDACTED]

Dear [REDACTED]

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (as amended, October 26, 2001), you are hereby directed to provide the Federal Bureau of Investigation (FBI) the names, addresses, lengths of service and electronic communication transactional records, to include existing transaction/activity logs and all e-mail header information (not to include message content and/or subject fields), for the below-listed email address:

[REDACTED]

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and 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.

You are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

You are requested to provide records responsive to this request personally to a representative of the [REDACTED] of the FBI. Any questions you have regarding this request should be directed only to the [REDACTED]. Due to security considerations, you should neither send the records through the mail nor disclose the substance of this request in any telephone conversation.



Your cooperation in this matter is greatly appreciated.

Sincerely,

A handwritten signature in cursive script, appearing to read "M. Bowman".

Marion E. Bowman  
Senior Counsel  
National Security Affairs  
Office of the General Counsel

**EXHIBIT B**

Mr. Nicholas Merrill

Page 3

ATTACHMENT

"In preparing your response to this request, you should determine whether your company maintains the following types of information which may be considered by you to be an electronic communication transactional record in accordance with Title 18, United States Code, Section 2709:

- [Redacted]
- Subscriber name [Redacted]
- Account number [Redacted]
- [Redacted]
- Address [Redacted]
- [Redacted] telephone number [Redacted]
- [Redacted]
- [Redacted]
- Billing [Redacted]
- [Redacted]
- e-mail address [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- Any other information which you consider to be an electronic communication transactional record

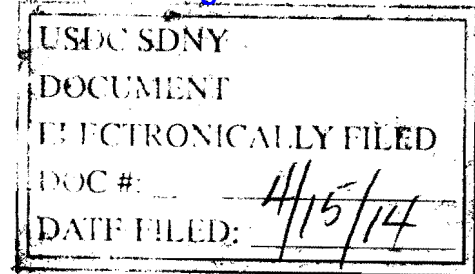
We are not requesting, and you should not provide, information pursuant to this request that would disclose the content of any electronic communication as defined in Title 18, United States Code, Section 2510(8)."



# **EXHIBIT C**



# **EXHIBIT A**



UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

----- X  
JOHN DOE, INC.; JOHN DOE; AMERICAN  
CIVIL LIBERTIES UNION; and AMERICAN  
CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs,

v.

ERIC HOLDER, JR., in his official capacity as  
Attorney General of the United States; JAMES B.  
COMEY, in his official capacity as Director of  
the Federal Bureau of Investigation; and JAMES  
A. BAKER, in his official capacity as General  
Counsel of the Federal Bureau of Investigation,

Defendants.<sup>1</sup>  
----- X

04 Civ. 2614 (VM)

**Stipulation and Order Modifying  
July 30, 2010, Judgment of Dismissal**

WHEREAS, in 2004, the Federal Bureau of Investigation (the "FBI") delivered a national security letter (the "Doe NSL") issued under 18 U.S.C. § 2709 to plaintiff John Doe, Inc., and its then-president, plaintiff John Doe. Pursuant to 18 U.S.C. § 2709, the Doe NSL sought certain information from its recipients. The Doe NSL included a page titled "Attachment," further specifying the information being sought (the "Attachment"). The Doe NSL further notified its recipients that 18 U.S.C. § 2709 prohibited its recipients from disclosing the fact that the FBI had sought or obtained access to information or records under that statute.

WHEREAS, plaintiffs John Doe, Inc., and John Doe refused to comply with the Doe NSL, and filed this action, challenging the Doe NSL, against defendants (the "government") in this Court on or about April 6, 2004. By Decision and Order entered September 6, 2007, this Court granted in part and denied in part plaintiffs' motion for summary judgment, and denied the government's cross-motion for dismissal or summary judgment. The government appealed, and the Court of Appeals for the Second Circuit, by opinion dated December 15, 2008, affirmed in part, reversed in part, and remanded the case for further proceedings.

WHEREAS, on remand, this Court considered the parties' cross-motions addressing whether the government was justified in continuing to impose a nondisclosure obligation on plaintiffs with respect to certain aspects of the Doe NSL.

WHEREAS, by Decision and Order dated October 20, 2009, this Court granted in part the government's motion for summary judgment and denied in part plaintiffs' motion for partial

<sup>1</sup> Pursuant to Fed. R. Civ. P. 25(d), the names of public officers have been automatically substituted for their predecessors.

summary judgment. By Decision and Order entered March 18, 2010, the Court granted in part and denied in part plaintiffs' motion for partial reconsideration.

WHEREAS, in particular, the March 18, 2010, Decision and Order considered the nondisclosure obligation as it related to the Attachment, directing the government to disclose certain information in the Attachment but also concluding that the nondisclosure obligation could continue to apply to other portions of the Attachment. In accordance with this order, the government provided plaintiffs with a redacted version of the Attachment (the "Redacted Attachment"), which is now in the public domain.

WHEREAS, plaintiffs appealed the March 18, 2010, Decision and Order, then later withdrew the appeal.

WHEREAS, by Stipulation and Order entered by the Court on July 30, 2010, plaintiffs and the government agreed to dismiss this action, and to partially set aside, but partially retain, the nondisclosure obligation set forth in 18 U.S.C. § 2709 as it pertains to the Doe NSL.

WHEREAS, due to changed circumstances, the FBI no longer believes that the nondisclosure of information in the Doe NSL—with the exception of non-public information in the Attachment—is necessary to prevent against a danger to the national security of the United States; interference with a criminal, counterterrorism, or counterintelligence investigation; interference with diplomatic relations; or danger to the life or physical safety of any person that is related to an authorized investigation to protect against international terrorism or clandestine intelligence activities.

WHEREAS, this Court has the authority to modify the July 30, 2010, Stipulation and Order pursuant to Fed. R. Civ. P. 60(b), and the parties consent to such modification upon the terms set forth below.

NOW, THEREFORE, IT IS HEREBY STIPULATED AND AGREED, by and between the parties, as follows:

1. The nondisclosure obligation set forth in 18 U.S.C. § 2709 continues to apply to the Attachment to the Doe NSL, except insofar as the information in the Attachment has already been made public in the Redacted Attachment.
2. Except as provided in paragraph 1 of this Stipulation and Order, the nondisclosure obligation set forth in 18 U.S.C. § 2709, as it pertains to the Doe NSL, is no longer in effect.
3. Nothing in this Stipulation and Order affects whatever rights plaintiffs John Doe and John Doe, Inc., may have to petition in the future under 18 U.S.C. § 3511(b) or any other provision of law for an order modifying or setting aside the nondisclosure requirement left in place by this Stipulation and Order.
4. This Stipulation constitutes the entire agreement of the parties, and no prior statement, representation, agreement, or understanding, oral or written, will have any force or effect.

Dated: New Haven, Connecticut  
April 11, 2014

MEDIA FREEDOM AND  
INFORMATION ACCESS CLINIC,  
YALE LAW SCHOOL  
Attorney for Plaintiffs John Doe and  
John Doe, Inc.

By: 

JONATHAN M. MANES  
P.O. Box 208215  
New Haven, Connecticut 06520  
Telephone: 203.432.9387  
E-mail: jonathan.manes@yale.edu

Dated: New York, New York  
April 11, 2014

PREET BHARARA  
United States Attorney for the Southern  
District of New York  
Attorney for Defendants

By: 

BENJAMIN H. TORRANCE  
86 Chambers Street  
New York, New York 10007  
Telephone: 212.637.2703  
E-mail: benjamin.torrance@usdoj.gov

SO ORDERED.

Dated: New York, New York  
15 April, 2014

  
VICTOR MARRERO, U.S.D.J.

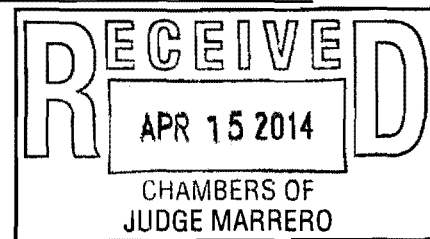


**U.S. Department of Justice**

*United States Attorney  
Southern District of New York*

86 Chambers Street  
New York, New York 10007

April 11, 2014



By hand

The Honorable Victor Marrero  
United States District Judge  
United States Courthouse  
500 Pearl Street  
New York, New York 10007

Re: *Doe v. Holder*, 04 Civ. 2614 (VM)


Dear Judge Marrero:

The parties to the above-named case have entered into the enclosed stipulation to modify this Court's prior order. We respectfully request that the Court so-order the stipulation.

Respectfully,

PREET BHARARA  
United States Attorney

By:

  
BENJAMIN H. TORRANCE  
Assistant United States Attorney  
Telephone: 212.637.2703  
Fax: 212.637.2702  
E-mail: benjamin.torrance@usdoj.gov

Encl.

cc: Anjali Motgi & Jonathan Manes, by email

## **EXHIBIT B**



**Subject:** Nicholas Merrill's NSL Gag Order  
**Date:** Wednesday, January 15, 2014 at 5:06:38 PM Eastern Standard Time  
**From:** Motgi, Anjali  
**To:** jeffrey.oestericher@usdoj.gov, benjamin.torrance@usdoj.gov  
**CC:** Manes, Jonathan, Victor, Jacob, Megre, Iya

Dear Mr. Oestericher and Mr. Torrance,

My name is Anjali Motgi, and I am writing on behalf of the Media Freedom and Information Access Clinic ("MFIA") at Yale Law School. We are currently representing Nicholas Merrill, recipient of an FBI National Security Letter in 2004. You may recall that Mr. Merrill, represented by Jameel Jaffer of the American Civil Liberties Union, previously challenged the NSL and the accompanying gag order that was imposed on him pursuant to 18 U.S.C § 2709(c). After lengthy litigation that case ended with a Stipulation, dated July 30, 2010, permitting Mr. Merrill to identify himself as the recipient of the NSL, and also preserving his right to challenge the remaining elements of the gag order in the future. See *Doe v. Holder*, No. 04-cv-2614 (S.D.N.Y. July 30, 2010), ECF No. 204.

Mr. Merrill continues to be subject to a gag order forbidding him from speaking about various aspects of the NSL, even though a decade has now elapsed since the NSL was issued, and more than three years have passed since the 2010 Stipulation, during which time there has been a great deal of public discussion regarding the FBI's NSL authority. Mr. Merrill has retained the MFIA Clinic to renew his challenge to the remaining portions of the gag. MFIA is a clinic at Yale Law School in which law students engage in practice under the supervision of attorneys David A. Schulz and Jonathan M. Manes. We are prepared to initiate renewed litigation on Mr. Merrill's behalf soon.

Before commencing litigation, however, we would like to schedule a time to speak with you to discuss the possibility that the government might voluntarily lift all or part of the gag, and thereby avoid the need for further litigation. It is our understanding that you were the attorneys assigned to the case at the time it was closed and are therefore most likely to be familiar with the file, which is why we have directed this correspondence to you. We would like to schedule a call or meeting no later than the end of the month of January; please feel free to propose a few dates and times that would work for you.

Thank you very much for your cooperation.

Sincerely,

Anjali Motgi  
Third Year Law Student and Clinic Member

cc: Jonathan Manes, Clinic Supervisor; Iya Megre and Jacob Victor, Clinic Members

Media Freedom and Information Access Clinic  
Yale Law School  
P.O. Box 208215

New Haven, CT 06520  
Tel: (203) 432-9387

# **EXHIBIT C**

*MARRINO 5*

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

----- X  
JOHN DOE, INC.; JOHN DOE; AMERICAN  
CIVIL LIBERTIES UNION; and AMERICAN  
CIVIL LIBERTIES UNION FOUNDATION,

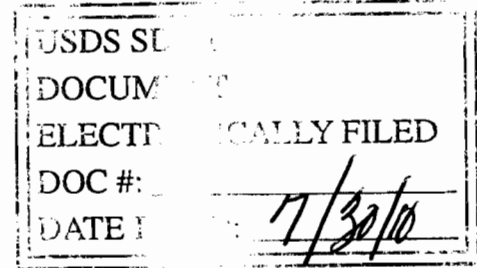
Plaintiffs,

v.

ERIC HOLDER, JR., in his official capacity as  
Attorney General of the United States; ROBERT  
MUELLER, III, in his official capacity as  
Director of the Federal Bureau of Investigation;  
and VALERIE E. CAPRONI, in her official  
capacity as General Counsel of the Federal  
Bureau of Investigation,

Defendants.  
----- X

04 Civ. 2614 (VM)



**STIPULATION AND ORDER OF DISMISSAL OF ACTION**

WHEREAS, plaintiffs-appellants ("Plaintiffs") filed this action against defendants-appellees (the "Government") in district court on or about April 6, 2004.

WHEREAS, by Decision and Order dated September 6, 2007, this Court granted in part and denied in part Plaintiffs' motion for summary judgment, and denied the Government's cross-motion for dismissal or summary judgment.

WHEREAS, the Government appealed and the Second Circuit Court of Appeals, by Order dated December 15, 2008, affirmed in part, reversed in part, and remanded the case for further proceedings.

WHEREAS, on remand, this Court considered the parties' cross-motions addressing whether the Government was justified in continuing to impose a non-disclosure obligation on

plaintiffs with respect to certain aspects of the National Security Letter (“NSL”) served upon plaintiff Doe, including Doe’s identity and certain parts of the Attachment to the NSL.

WHEREAS, by Decision and Order dated October 20, 2009, this Court granted in part the Government’s motion for summary judgment and denied in part Plaintiffs’ motion for partial summary judgment. In so ruling, the Court held that the Government had carried its burden of demonstrating that continuation of the requirement imposed on Plaintiffs not to disclose certain aspects of the NSL, including Doe’s identity and certain parts of the Attachment, was justified.

WHEREAS, Plaintiffs moved for partial reconsideration of the October 20, 2009 Decision and Order insofar as it pertained to the Attachment to the NSL.

WHEREAS, by Decision and Order entered March 18, 2010, this Court granted in part and denied in part Plaintiffs’ motion for partial reconsideration, directed the Government to supply a less-redacted, public version of the NSL consistent with the Court’s rulings, and directed the Clerk of Court to close this case.

WHEREAS, on May 17, 2010, Plaintiffs filed a Notice of Appeal from this Court’s October 20, 2009 and March 18, 2010 Decisions and Orders.

WHEREAS, due to a change in circumstances, the FBI no longer believes that non-disclosure of the identity of the recipient of the NSL is necessary to prevent against a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person that is related to an authorized investigation to protect against international terrorism or clandestine intelligence activities.

WHEREAS, as a result of a settlement reached by the parties on July 26, 2010, the parties filed a Stipulation in the Second Circuit Court of Appeals providing, inter alia, that plaintiffs' appeal from this Court's October 20, 2009 and March 18, 2010 Decisions and Orders (Docket No. 10-2052) was withdrawn subject to reinstatement by September 20, 2010. The Stipulation was "So Ordered" on July 28, 2010, and a certified copy was issued on that same day.

WHEREAS, the parties wish to resolve this matter, thereby avoiding further proceedings and expense, under the terms set forth below.

NOW, THEREFORE, IT IS HEREBY STIPULATED AND AGREED, by and between the parties, as follows:

1. The above-captioned action shall be, and hereby is, dismissed with prejudice pursuant to Rule 41(a)(2) of the Federal Rules of Civil Procedure.
2. Plaintiffs hereby agree that they will not reinstate their appeal from this Court's October 20, 2009 and March 18, 2010 Decisions and Orders (Docket No. 10-2052).
3. Plaintiff John Doe is hereby permitted to identify himself and his company as the recipient of the NSL that has been the subject of this litigation. Plaintiffs ACLU and ACLU Foundation may publicly disclose this information as well. In addition, the Government acknowledges that plaintiffs may discuss matters and information that have been filed without redaction on the public docket in this case.
4. Plaintiffs are also permitted to publicly discuss plaintiff Doe's personal background, background about his company, the services Doe generally provided to his clients, and his type of clientele generally, including (a) the information that is redacted in the public filing of the Third Declaration of John Doe, dated August 21, 2009, Paragraph 1; (b) the

information that is redacted in the public filing of the Second Declaration of John Doe, dated September 8, 2006, Paragraph 4; and (c) the information that is redacted in the public filing of the Second Declaration of John Doe, dated September 8, 2006, Paragraph 37.

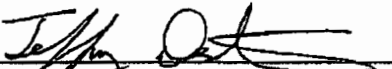
5. Except as expressly stated in paragraphs 3 and 4 above and in this Court's prior Orders in this case, the non-disclosure requirement set forth in 18 U.S.C. § 2709 continues to apply with respect to the NSL issued to plaintiff Doe. Similarly, except as expressly stated in paragraphs 3 and 4 above and in this Court's prior Orders in this case, all material that was filed under seal or was redacted from the public record and never subsequently filed unredacted on the public docket in this case must be kept confidential and may not be publicly disclosed.

6. Nothing in this Stipulation shall affect plaintiff Doe's right and plaintiffs ACLU and ACLU Foundation's right, if any, to petition in the future under 18 U.S.C. § 3511(b) for an order modifying or setting aside the nondisclosure requirement imposed in connection with the NSL served on plaintiff Doe.

7. This Stipulation constitutes a final judgment in this action and contains the entire agreement of the parties, and no prior statement, representation, agreement, or understanding, oral or written, that is not contained herein, will have any force or effect.

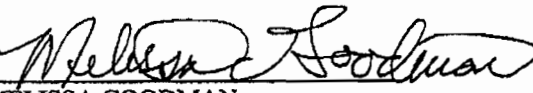
Dated: New York, New York  
July 29, 2010

PREET BHARARA  
United States Attorney for the  
Southern District of New York  
Attorney for Defendants

By:   
JEFFREY S. OESTERICHER  
BENJAMIN H. TORRANCE  
Assistant United States Attorneys  
86 Chambers Street  
New York, New York 10007  
Telephone: 212.637.2698, .2703  
Fax: 212.637.2730  
E-mail: [jeffrey.oestericher@usdoj.gov](mailto:jeffrey.oestericher@usdoj.gov)  
[benjamin.torrance@usdoj.gov](mailto:benjamin.torrance@usdoj.gov)

Dated: New York, New York  
July 29, 2010

AMERICAN CIVIL LIBERTIES FOUNDATION  
Attorneys for Plaintiffs

By:   
MELISSA GOODMAN  
JAMEEL JAFFER  
125 Broad Street, 18<sup>th</sup> Floor  
New York, New York 10004  
Telephone: (212) 549-2622  
Fax: (212) 549-2654  
E-mail: [mgoodman@aclu.org](mailto:mgoodman@aclu.org)

SO ORDERED: 30 July 2010

  
Victor Marrero  
United States District Judge



# **EXHIBIT D**

**Subject:** Following up about Nicholas Merrill's NSL gag order

**Date:** Sunday, February 2, 2014 at 10:29:17 AM Eastern Standard Time

**From:** Motgi, Anjali

**To:** benjamin.torrance@usdoj.gov, jeffrey.oestericher@usdoj.gov

**CC:** Manes, Jonathan, dschulz@lskslaw.com, Victor, Jacob, Graham, Benjamin

Dear Mr. Torrance and Mr. Oestericher,

I hope this email finds you well. I am writing to follow up with you about my email of January 15 regarding Nicholas Merrill's ongoing NSL gag order. January has now drawn to a close with no substantive response; we would like to discuss as soon as possible whether the FBI will drop the remaining portions of Mr. Merrill's NSL gag order. It may be worth noting that two days after we sent you our email, the President spoke directly on this issue at some length, and specifically "directed the Attorney General to amend how we use national security letters so that this secrecy will not be indefinite, so that it will terminate within a fixed time unless the government demonstrates a real need for further secrecy." As you know, Mr. Merrill has now been subject to the FBI's gag order for ten years.

Please let us know if you would be free to speak with us by telephone this week.

Thank you,  
Anjali

Anjali Motgi  
Media Freedom and Information Access Clinic  
Yale Law School | [anjali.motgi@clinics.yale.edu](mailto:anjali.motgi@clinics.yale.edu)

## **EXHIBIT D**

**EXHIBIT E**

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE

Date: 11/28/2001

To: All Field Offices

Attn: ADIC;  
SAC;  
CDC  
FCI/IT Supervisors  
AD Watson;  
DADs;  
Section Chiefs  
AD Gallagher;  
DADs;  
Section Chiefs

Counterterrorism

National Security

From: General Counsel

National Security Law Unit, Room 7975

Contact: [Redacted]

Approved By: Mueller Robert S III  
Pickard Thomas J  
Parkinson Larry R  
Bowman M E

b7C

Drafted By: [Redacted] :mjw  
R Jr:jrl

Case ID #: 66F-HQ-A1255972

Title: NATIONAL SECURITY LETTER MATTERS

Synopsis: Provides guidance on the preparation, approval, and service of National Security Letters (NSLs).

Reference: 66F-HQ-A1255972 Serial 15

- Enclosure(s):
- 1) Subscriber Information NSL Model
  - 2) Toll Billing Records NSL Model
  - 3) Electronic Subscriber Information NSL Model
  - 4) Electronic Communication Transactional Records NSL Model
  - 5) Financial Records NSL Model
  - 6) Identity of Financial Institutions NSL Model
  - 7) Consumer Identifying Information NSL Model
  - 8) Subscriber/Electronic Subscriber (EC) Model
  - 9) Toll/Transactional Records EC Model
  - 10) Financial Records EC Model
  - 11) Financial Institutions/Consumer Identity EC Model
  - 12) ECPA NSL Checklist
  - 13) RFPA NSL Checklist

11-6-02  
ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-6-02 BY 60267 NCS/EP/CLT  
#966750

To: All Field Offices From: General Counsel  
Re: 66F-HQ-A1255972, 11/28/2001

14) FCRA NSL Checklist

**Details:** In the referenced communication, dated 11/09/2001, the Director of the FBI delegated the authority to certify NSLs to the following officials: (1) the Deputy Director; (2) The Assistant Directors (ADs) and all Deputy Assistant Directors (DADs) of the Counterterrorism Division (CTD) and the National Security Division (NSD); (3) the General Counsel and the Deputy General Counsel for National Security Affairs (DGC), Office of the General Counsel (OGC); (4) the Assistant Director in Charge (ADIC), and all Special Agents in Charge (SACs), of the New York, Washington, D.C., and Los Angeles field divisions; and (5) the SACs in all other field divisions. The purpose of this electronic communication is to provide comprehensive guidance on the preparation, approval, and service of NSLs.

1. Introduction to National Security Letters

NSLs are administrative subpoenas that can be used to obtain several types of records. There are three types of NSLs. First, pursuant to the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709, the FBI can issue NSLs for: (1) telephone subscriber information (limited to name, address, and length of service); (2) telephone local and long distance toll billing records; and (3) electronic communication transactional records. Second, pursuant to the Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3414(a)(5), the FBI can issue NSLs to obtain financial records from banks and other financial institutions. Finally, pursuant to the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681u, the FBI can issue NSLs to obtain consumer identifying information and the identity of financial institutions from credit bureaus.

NSLs are tools available in investigations conducted under the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG). The FCIG currently provide that an NSL can be issued during the course of a full international terrorism or foreign counterintelligence investigation. **NSLs cannot be used in criminal investigations unrelated to international terrorism or clandestine intelligence activities.** Given the new statutory language, the OGC and DOJ have taken the position that NSLs also may be authorized in foreign counterintelligence (FCI) and international terrorism (IT) preliminary inquiries (PIs), with prior coordination through the relevant NSD or CTD unit at FBIHQ. This position is based on the conclusion that all investigations authorized under the FCIG, including PIs, are to "protect against international terrorism or clandestine intelligence activities," as required by the NSL statutory authorities. At present, however, issuing an NSL in the context of a PI will require a

To: All Field Offices From: General Counsel  
Re: 66F-HQ-A1255972, 11/28/2001

waiver or modification of the FCIG. Obtaining such a waiver currently is possible only in international terrorism cases. The FCIG are being revised, but this revision may take some time. Thus, whenever the information sought is relevant to an established full investigation, the field likely will find it more efficient to issue an NSL out of the related full investigation than to request one in a PI.

2. General Policy on the Use of NSL Authority

NSLs are powerful investigative tools, in that they can compel the production of substantial amounts of relevant information. However, they must be used judiciously. The USA PATRIOT Act greatly broadened the FBI's authority to gather this information. However, the provisions of the Act relating to NSLs are subject to a "sunset" provision that calls for the expiration of those provisions in four years. In deciding whether or not to re-authorize the broadened authority, Congress certainly will examine the manner in which the FBI exercised it. Executive Order 12333 and the FCIG require that the FBI accomplish its investigations through the "least intrusive" means. Supervisors should keep this in mind when deciding whether or not a particular use of NSL authority is appropriate. The greater availability of NSLs does not mean that they should be used in every case.

In addition, the removal of any requirement for FBIHQ coordination in the issuing of NSLs creates the possibility of duplicate requests for the same information by different field offices. Field offices must take steps to avoid this. In particular, the field should check FBI databases (ACS, Telephone Application, etc.) and open sources to see if the information sought has already been obtained by the FBI or whether it is publically available. This is particularly important when considering issuing NSLs for telephone or electronic communications data under the Electronic Communications Privacy Act (ECPA). Unlike the criminal authorities in ECPA, the NSL authority does not require the government to reimburse carriers or Internet Service Providers (ISPs) for the cost of producing the requested information. A dramatic increase in duplicate NSLs will only augment existing pressure to require governmental reimbursement.

Individual field offices have the responsibility for establishing and enforcing an appropriate review and approval process for the use of NSL authorities.

To: All Field Offices From: General Counsel  
Re: 66F-HQ-A1255972, 11/28/2001

### 3. The Mechanics of Producing NSLs

For all types of NSLs, the issuing office needs to prepare two documents: (1) the NSL itself; and (2) an EC approving the NSL and documenting the predication. Model NSLs and ECs for all variations of the three types of NSLs are included as attachments to this communication. These materials will also be placed on the NSLU Intranet Website and will be distributed by GroupWise e-mail. Once the initial implementation of these new authorities is accomplished, NSLU will work to develop a macro or form to further streamline the NSL process.

#### A. The NSL

There are presently seven variations of the three NSL types: 1) subscriber information; 2) toll billing records; 3) electronic subscriber information; 4) electronic communication transactional records; 5) financial records; 6) identity of financial institutions; and 7) consumer identifying information. This section will discuss the features that these variations share in common and highlight the differences.

All NSLs must be addressed to an appropriate company point of contact. NSLU will place a list of known points of contact on its intranet website. However, the responsibility for ensuring that the company point of contact is up to date belongs to the drafting field division. Field divisions should advise NSLU of any new points of contact, or when a particular point of contact is no longer valid. Please note that the company point of contact address does not include a zip code, because NSLs must be hand-delivered.

The first paragraph of every NSL provides the appropriate statutory authority for the request, identifies the types of records requested, and provides available identifying information so that the company can process the NSL request. It is this first paragraph that contains the differences that warrant the seven NSL varieties.

Subscriber and electronic subscriber NSLs should have a specific date for each of the phone numbers/e-mail addresses requested. Typically, the specific date is going to be the date that the phone number or e-mail address was used in communication with the subject of the investigation. Any phone numbers identified in a subscriber request should contain all ten digits of the phone number, including the area code.

Toll billing record and electronic communication transactional record requests should have a range of dates for



To: All Field Offices From: General Counsel

Re: 66F-HQ-A1255972, 11/28/2001

each of the phone numbers/e-mail addresses requested. The date range may be from inception to present, or some other specified date range relevant to the investigation. Any phone numbers identified in a toll billing record request should contain all ten digits of the phone number, including the area code.

Financial record requests should include all available identifying information to facilitate the financial institution's records search. Typically, such identifying information includes: name, account numbers, social security number, and date of birth. The time period for financial record requests is typically from inception of account(s) to present, although a more specific date range may be used.

Credit record requests are similar to financial requests in that they should include available identifying information to facilitate the credit agency's records search. Typically, such identifying information includes: name, social security number, and date of birth. There is no need to specify a date range for credit record requests because these requests seek all records where the consumer maintains or has maintained an account.

The second paragraph of every NSL contains the statutorily required certification language. The certification language is virtually identical for every NSL. However, please note that the certification language used in the financial records NSLs is slightly different than the others in that it states "the records are sought for foreign counterintelligence purposes . . . ." Financial records also contain an additional certification that the FBI has complied with all applicable provisions of the RFPA. Use of the model NSLs will ensure that the proper certifications are made.

The next paragraph contains an admonition for the phone company, ISP, financial institution, or credit agency receiving the NSL. The paragraph warns that no officer, employee, or agent of the company may disclose that the FBI has sought or obtained access to the requested information or records.

The last substantive paragraph instructs the company point of contact to provide the records personally to a representative of the delivering field division. It also states that any questions should be directed to the delivering field division. This last paragraph requires the person preparing the NSL to input the appropriate delivering field division in two places.

The model NSLs for financial records and electronic communication transactional records each have a separate attachment. These attachments provide examples of information

To: All Field Offices From: General Counsel  
Re: 66F-HQ-A1255972, 11/28/2001

which the company might consider to be financial or electronic communication transactional records.

Finally, the NSL is an unclassified document because it does not detail the specific relevance of the requested records to an authorized FBI investigation. There is no need to classify the NSL when attaching it to the cover EC.

#### B. The Cover EC

The Cover EC serves four essential functions in the NSL process: (1) it documents the predication for the NSL by recording why the information sought is relevant to an investigation; (2) it documents the approval of the NSL by relevant supervisors and the legal review of the document; (3) it contains the information needed to fulfill the Congressional reporting requirements for each type of NSL; and (4) it transmits the NSL to the requesting squad or delivering field division for delivery to the appropriate telecommunications carrier, ISP, financial institution, or credit agency. There are four varieties of model ECs provided with this communication: (1) subscriber/electronic subscriber information; (2) toll billing/electronic communication transactional records; (3) financial records; and (4) credit information. When preparing an NSL request, the field should use one of these model ECs, giving special consideration to the elements discussed in this section.

##### 1) Field Descriptors

This section will generally explain how most of the EC field descriptors should be completed. The "**Precedence**" descriptor will typically be "ROUTINE." The "**Date**" descriptor should reflect the date the NSL and the EC were approved. The "**To**" descriptor will always include "General Counsel" and the requesting squad's field division. It may also include the name of the delivering field division (always Los Angeles in the case of FCRA NSLs) and the office of origin, if applicable. The "**Attn**" descriptor should include the name of the Chief, NSLU, and the squad supervisors and case agents from the requesting squad, delivering field division, and office of origin, if applicable and if known. The credit model EC identifies the FBI personnel working on Squad 4, Santa Ana RA, who are currently responsible for the service of FCRA NSLs. The "**From**" descriptor should identify the certifying official's field division, and include the title of the certifying official. The "**Contact**" descriptor should reflect the name and phone number of the requesting squad case agent. The "**Drafted By**" descriptor should reflect the name of the person who prepared the NSL package. The "**Case ID #**" descriptor must contain the case file number relevant to the

request, and the case file numbers indicated in the model EC. The "Title" descriptor should list the subject's name, any known aliases, whether the investigation is an FCI or IT investigation directed at a particular foreign power, and identify the office of origin, e.g., WILLIAM BADGUY, AKA BILL BADGUY, FCI-IRAQ, OO: NEW YORK. The "Synopsis" descriptor should use the standard boilerplate contained in the appropriate model EC. The "Derived From" descriptor should be "G-3" in bold typeface. The "Declassify On" descriptor should be "X1" in bold typeface. the "Full Investigation Instituted" descriptor should contain the date the full FCI or IT investigation was opened on the subject and indicate whether the subject is a U.S. person. Please note that the word "Field" has been deleted from the field descriptor contained in the standard EC macro. In the unlikely event that an NSL is issued during a PI with prior FBIHQ approval, the field descriptor should be edited to state "Preliminary Inquiry Instituted." The remaining descriptors can be filled in according to the model EC being used.

## 2) Predication and Relevance

The USA PATRIOT Act has greatly simplified the NSL process. The FBI official authorizing the issuance of an NSL is no longer required to certify that there are specific and articulable facts giving reason to believe that the information sought pertains to a foreign power, or an agent of a foreign power. NSLs may now be issued upon a certification of relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities.

Accordingly, the first paragraph in the "Details" section of the EC should contain the predication for the full investigation and identify the relevance of the requested records to the investigation. Both the predication and relevance should be stated clearly and concisely. The predication should track with the predicates contained in FCIG, Section III.C.1. For example, the predication might state, "A full foreign counterintelligence investigation of subject, a Non-U.S. person, was authorized in accordance with the Attorney General Guidelines because he may be a suspected intelligence officer for the Government of Iraq." Another example might state, "A full international terrorism investigation of subject, a U.S. person, was authorized in accordance with the Attorney General Guidelines because he may be engaged in international terrorism activities by raising funds for HAMAS."

The relevance requirement ties the requested records to the appropriate full investigation. For example, relevance could be established by stating, "This subscriber information is being

To: All Field Offices From: General Counsel  
Re: 66F-HQ-A1255972, 11/28/2001

requested to determine the individuals or entities that the subject has been in contact with during the past six months." Another example might state, "The subject's financial records are being requested to determine his involvement in possible HAMAS fund raising activities."

3) Approval

The second paragraph in the "Details" section and the "Approved By" descriptor field of the EC should reflect the level of the official approving the issuance of the EC and signing the NSL's certification. Prior to certification, every NSL and cover EC issued by the field division should be reviewed by the squad supervisor, the Office of the Chief Division Counsel, and the ASAC. Lawyers reviewing NSL packages should use the checklists provided with this communication to ensure legal sufficiency. The last step in the approval process occurs when the certifying official (Deputy Director, ADs, General Counsel, ADICs, DADs, DGC, or SACs) personally signs the NSL and initials the EC. Certifying officials may not further delegate signature authority.

4) Reporting Requirements

NSLU will continue to prepare the mandatory reports to Congress required for each NSL type. To ensure that NSLU receives sufficient information to prepare these reports, it is critical that the person preparing the NSL package follow the NSL and EC models very carefully. The second lead in every model EC requests NSLU to "record the appropriate information needed to fulfill the Congressional reporting requirements for NSLs." NSLU will be able to compile the reporting data provided that the cover EC includes the case file number, the subject's U.S. person status, the type of NSL issued, and the number of phone numbers, e-mail addresses, account numbers, or individual records being requested in the NSL. Once NSLU has entered this reporting data into its NSL database, it will clear the lead set in the cover EC.

5) Transmittal

Often, the squad requesting the NSL will be able to hand-carry the NSL locally to the appropriate company point of contact. However, in many situations, the field division drafting the NSL will have to get it delivered by another field division. In these situations, the drafting division should attempt to identify the squad and personnel at the delivering field division who will be responsible for delivering the NSL. In the event that the office of origin is different than either

To: All Field Offices From: General Counsel  
Re: 66F-HQ-A1255972, 11/28/2001

the drafting division or delivering division, the person drafting the NSL package should ensure that the case agent from the office of origin receives a copy of the package. The first lead in the model ECs should direct the requesting squad or delivering field division to deliver the attached NSL. If the delivering division is different than the drafting division or the office of origin, then this first lead should also request the delivering division to submit the results to the drafting division and/or the office of origin.

4. NSL Preparation Assistance

Some field divisions may, for a variety of reasons, opt not to exercise their delegated authority to issue NSLs. Other field divisions may exceed their capacity to issue NSLs and seek assistance in handling the overflow. NSLU will continue to process any NSL request that it receives. Field divisions should send their requests directly to NSLU, with information copies to the FBIHQ substantive unit. Such requests must contain all the information identified in this communication as necessary to prepare the NSL package. NSLU anticipates that it will be able to process such requests within one to three business days.

Any questions regarding this communication may be directed to [redacted] NSLU, OGC, at [redacted]

b7C

**EXHIBIT F**

**U.S. Department of Justice**  
Office of the Inspector General

---

# A Review of the Federal Bureau of Investigation's Use of National Security Letters: *Assessment of Progress in Implementing Recommendations and Examination of Use in 2007 through 2009*



Office of the Inspector General  
Oversight and Review Division  
August 2014

---

**UNCLASSIFIED**

**TABLE OF CONTENTS**

EXECUTIVE SUMMARY..... vii

I. Current Status of Implementation of Recommendations Made in the  
OIG’s First and Second NSL Reports ..... viii

II. FBI’s Use of National Security Letters During Calendar Years 2007,  
2008, and 2009..... ix

III. Current Status of Implementation of Recommendations Made in the  
OIG’s Exigent Letters Report ..... xii

IV. Conclusion..... xiv

CHAPTER ONE: INTRODUCTION..... 1

I. The FBI’s Authority to Issue National Security Letters ..... 2

II. Methodology of the OIG Review ..... 5

III. Organization of this Report..... 7

CHAPTER TWO: STATUS OF THE FBI’S AND THE DEPARTMENT’S  
CORRECTIVE ACTIONS IN RESPONSE TO THE OIG’S FIRST AND  
SECOND NSL REPORTS ..... 9

I. Overview of the OIG’s Previous Findings and the FBI’s and the  
Department’s Corrective Measures ..... 10

II. Status of the FBI’s and the Department’s Implementation of the OIG’s  
Recommendations..... 16

A. Internal Controls ..... 16

B. Guidance and Training ..... 25

C. Record-keeping..... 36

D. Oversight..... 46

III. Conclusions and Recommendations ..... 52

CHAPTER THREE: REVIEW OF THE FBI’S USE OF NATIONAL SECURITY  
LETTERS IN 2007 THROUGH 2009..... 55

I. National Security Letter Requests in 2007 through 2009 ..... 55

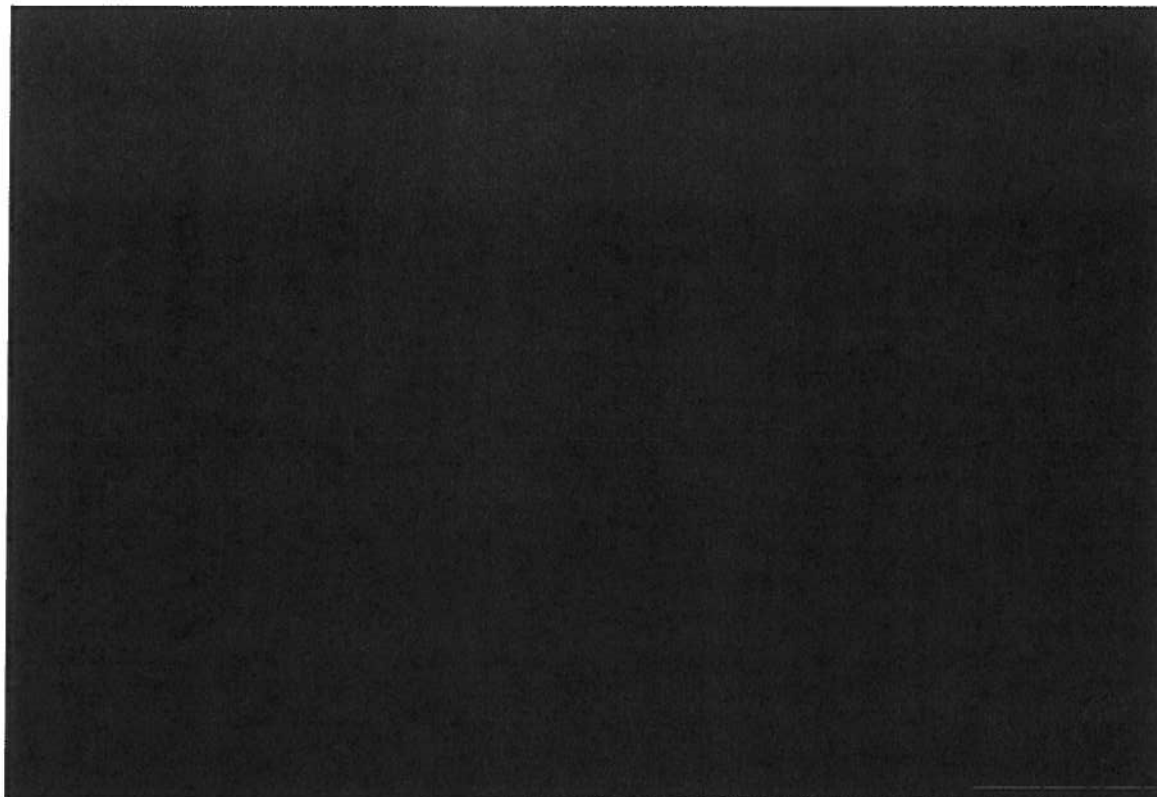
A. Methodology ..... 59



B.	Description of National Security Letter Requests in 2007 through 2009 .....	59
C.	Trends in National Security Letter Usage from 2003 through 2009 .....	64
II.	Usefulness of National Security Letters as an Investigative Tool .....	67
A.	National Security Letters as an Investigative Tool.....	67
B.	National Security Letter Requests for Electronic Communication Transactional Records .....	70
CHAPTER FOUR: OIG FINDINGS ON THE FBI’S COMPLIANCE WITH NSL REQUIREMENTS IN 2008 AND 2009 .....		75
I.	Potential IOB Violations Reported to FBI OGC Arising From National Security Letters .....	76
A.	IOB Reporting Criteria .....	76
B.	NSL-Related Potential IOB Violations Reported to the FBI OGC....	79
C.	NSL-Related Potential IOB Violations Reported to the IOB .....	81
D.	OIG Analysis of the Reporting of Potential IOB Violations to the IOB .....	88
E.	NSL-related Potential IOB Violations Not Reported to the IOB .....	90
F.	OIG Analysis of NSL-related Potential IOB Violations Not Reported to the IOB.....	94
II.	The Findings of the FBI Inspection Division’s NSL Reviews and the Department’s National Security Reviews in 2008 and 2009 .....	102
A.	2008 and 2009 FBI Inspection Division NSL Reviews.....	103
1.	Methodology.....	103
2.	FBI Inspection Division’s Findings.....	104
3.	FBI Inspection Division’s Recommendations.....	109
4.	OIG Analysis.....	116
B.	2007-2009 National Security Reviews.....	118
1.	NSR Methodology .....	118
2.	National Security Review Findings.....	120
3.	Other Issues Identified in National Security Reviews .....	123
4.	OIG Analysis.....	125
III.	OIG Review .....	125
A.	Methodology of the OIG Review.....	125
B.	Failures to Comply with NSL Requirements .....	126

1.	Potential IOB Violation Identified by the OIG .....	126
2.	NSL-Related Compliance Failures.....	127
C.	OIG Analysis.....	136
IV.	OIG Conclusions and Recommendations .....	140
CHAPTER FIVE: OTHER NOTEWORTHY ISSUES RELATED TO THE FBI'S USE OF NATIONAL SECURITY LETTERS .....		145
I.	Telephone Toll Billing Records.....	145
A.	Telephone Records Obtained Through TCAU.....	147
1.	Background .....	147
2.	Telephone Records Obtained by the TCAU in Response to NSLs .....	150
3.	FBI OGC Guidance.....	152
B.	Personal Information Other Than Name, Address, and Length of Service.....	154
C.	"Associated" Telephone Records .....	157
D.	Conclusion .....	159
II.	Handling of NSL Return Data Received Post-Investigation .....	160
III.	Recommendations.....	161
CHAPTER SIX: STATUS OF THE FBI'S AND THE DEPARTMENT'S CORRECTIVE ACTIONS IN RESPONSE TO THE OIG'S EXIGENT LETTERS REPORT .....		163
I.	Status of the Implementation of the OIG's Recommendations .....	165
II.	Conclusions and Recommendations .....	185
CHAPTER SEVEN: CONCLUSIONS AND RECOMMENDATIONS .....		187
APPENDICES .....		

**[ Pages iv – xiv; 1 – 63 omitted ]**

**FIGURE 3.6: 2009 NSL Requests by NSL Type**

TTR = Toll Billing Records	FR = Financial Records
TSI = Telephone Subscriber Information	FIL = Financial Institution Listings
ECTR = Electronic Communication Transactional Records	CII = Consumer Identifying Information
ESI = Electronic Subscriber Information	FCR = Full Credit Reports

Source: Excel Spreadsheets provide by the FBI generated from the NSL subsystem

### **C. Trends in National Security Letter Usage from 2003 through 2009**

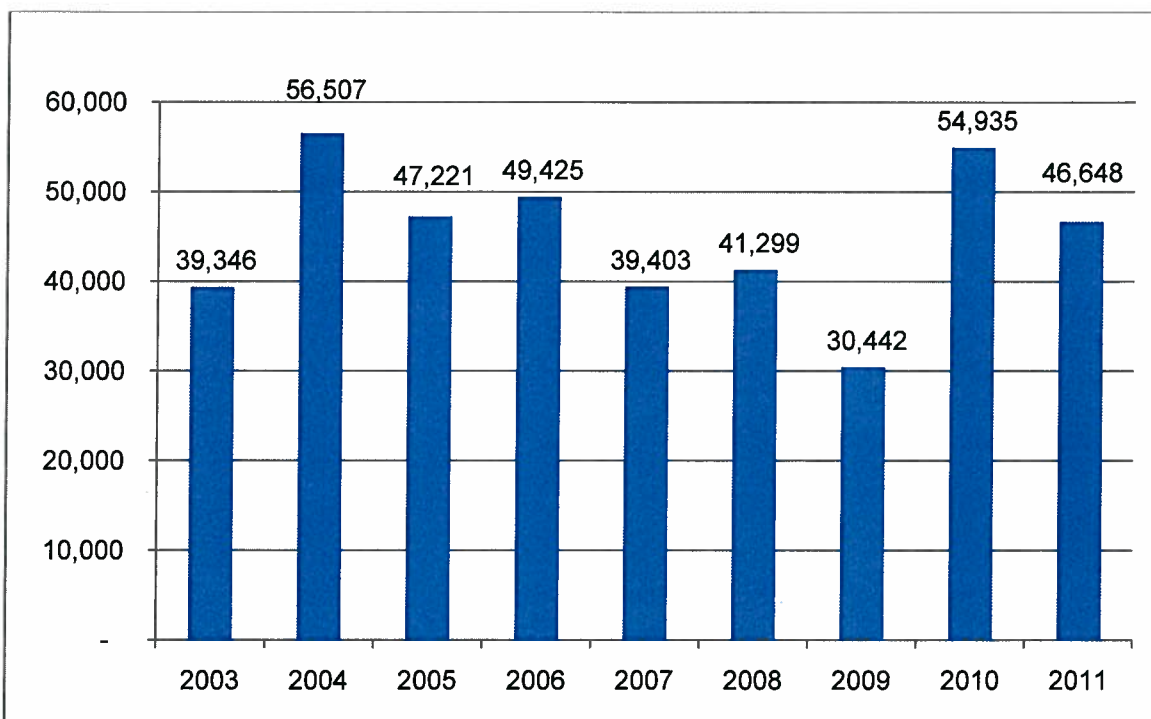
In this section, we describe the trends in the FBI's NSL requests from 2003 through 2009 as documented in the Department's semiannual classified reports to Congress, our review of the OGC database in our first and second NSL reviews, and in the NSL data provided to the OIG in this review, when applicable.

According to the Department's semiannual classified reports to Congress covering 2007 through 2009, the FBI issued a total of 111,144 NSL requests during 2007 through 2009. The individual totals for 2007, 2008, and 2009 varied as shown in Figure 3.1, and the average annual number of requests for the period was approximately 37,048. By comparison, the FBI issued approximately 51,051 NSLs per year between

2004 and 2006, and approximately 48,125 NSL requests per year between 2003 and 2006.<sup>78</sup> Thus, the FBI issued significantly fewer NSL requests during 2007 through 2009 than during 2003 through 2006.

The Department's most recent semiannual classified reports to Congress, however, indicate that the FBI's NSL use returned to historically typical numbers after 2009 – 54,935 NSL requests in 2010 and 46,648 in 2011.<sup>79</sup>

**FIGURE 3.7: NSL Requests 2003-2011**



Source: Semiannual Classified Congressional Reports

<sup>78</sup> In our second NSL report, we reported that the FBI issued a total of 192,499 NSL requests during 2003 through 2006. This number consisted of [REDACTED] requests reported to Congress in the Department's original semiannual classified reports covering 2003 through 2006 and [REDACTED] NSL requests for consumer full credit reports issued from 2003 through 2005 that the Department was not required to report to Congress. NSL II Report, at 109; NSL I Report, 36.

<sup>79</sup> See the Department's semiannual classified reports submitted to Congress on March 28, 2011 covering July 1, 2009, through December 31, 2010, the reports submitted on December 29, 2011, covering January 1, 2011, through June 30, 2011, and the reports submitted on February 8, 2012, for the semiannual periods covering July 1, 2011, through December 31, 2011.

The factors that may have contributed to the decrease in NSL usage from 2007 through 2009 as compared to previous years are not evident from the data we reviewed. Although the OIG requested an explanation from the FBI for the decrease in NSL usage during this period, the FBI represented that neither the Department nor the FBI had a process in place to identify the reasons for the change in NSL usage from year to year. According to the FBI, the number of NSLs issued in any given year is a function of the needs of the national security investigations conducted during that year.

During our field visits, we asked FBI personnel whether they had observed any changes in the FBI's or their own use of NSLs in the last five years. Most field personnel we interviewed told us that they had not observed any changes in NSL use. However, two supervisors and a division counsel told us that they believe agents use NSLs less often now than they did five years ago. These individuals told us that because of increased scrutiny on NSL use agents employ alternative investigative tools when possible. We have no information that these observations are representative of the experience in the field generally, and we note that the NSL data for 2010 and 2011 shown in Figure 3.7 does not indicate a continued trend of less frequent NSL use by the FBI.

Similarly, the data does not reveal the factors that contributed to the FBI issuing only 30,442 NSL requests in 2009, the lowest number of annual requests during the 9-year period depicted in Figure 3.7. Further, available information from the Department's semiannual classified reports indicates that during 2009, the FBI issued substantially fewer subscriber-only NSLs pursuant to the ECPA – only [REDACTED] as compared to [REDACTED] in 2008 and [REDACTED] in 2007. Steven Siegel, the former Deputy General Counsel of the FBI OGC's National Security Law Branch between September 2009 and April 2012, told us that 2009 was an "anomaly" from a statistical perspective and that the FBI would need to devote a substantial amount of resources to determine the reasons for the significant decrease in NSL use that year, an effort that the FBI has not undertaken.

Finally, the NSL data reflected in Figure 3.4 shows that well more than half of the FBI's NSL requests in 2007 through 2009 were generated from investigations of U.S. persons: 12,818, or 64 percent, in 2007; 18,447, or 74 percent, in 2008; and 13,515, or 63 percent, in 2009. This data indicates that the shift reported in our second NSL review toward more NSL requests generated from investigations of U.S. persons as compared to non-U.S. persons – from 39 percent in 2003 to 57 percent in 2006 – continued in 2007 through 2009.<sup>80</sup>

---

<sup>80</sup> NSL II Report, 110-112.

**[ Pages 67 – 196 and Appendices omitted ]**

# **EXHIBIT G**



~~TOP SECRET//NOFORN~~



# Office of the Director of National Intelligence

Statistical Transparency Report Regarding use of  
National Security Authorities

Annual Statistics for Calendar Year 2013

~~Classified By: 2381928  
Derived From: ODNI COL T-12  
Reason:  
Declassify On: 20391231~~

~~TOP SECRET//NOFORN~~

## **Statistical Transparency Report Regarding use of National Security Authorities**

June 26, 2014

### **Introduction.**

In June 2013, President Obama directed the Intelligence Community to declassify and make public as much information as possible about certain sensitive U.S. Government surveillance programs while protecting sensitive classified intelligence and national security information. Over the past year, the Director of National Intelligence (DNI) has declassified and authorized the public release of thousands of pages of documents relating to the use of critical national security authorities. Today, and consistent with the DNI's directive on August 29, 2013, we are releasing information related to the use of these important tools, and will do so in the future on an annual basis. Accordingly, the DNI has declassified and directed the release of the following information for calendar year 2013.

### **Annual Statistics for Calendar Year 2013 Regarding Use of Certain National Security Legal Authorities.**

#### **Titles I, III, IV, and VII of FISA.**

<b>Legal Authority</b>	<b>Annual Number of Orders</b>	<b>Estimated Number of Targets Affected</b>
FISA Orders based on probable cause (Title I and III of FISA, Sections 703 and 704 of FISA)	1,767 orders	1,144
Section 702 of FISA	1 order	89,138
FISA Pen Register/Trap and Trace (Title IV of FISA)	131 orders	319

It is important to provide some additional context to the above statistics.

- **Targets.** Within the Intelligence Community, the term "target" has multiple meanings. For example, "target" could be an individual person, a group, or an organization composed of multiple individuals or a foreign power that possesses or is likely to communicate foreign intelligence information that the U.S. government is authorized to acquire by the above-referenced laws. Some laws require that the government obtain a Court order specifying the communications facilities used by a "target" to be subject to intelligence collection. Although the government may have legal authority to conduct intelligence collection against multiple communications facilities used by the target, the user of the facilities - the "target" - is only counted once in the above figures.

~~TOP SECRET//NOFORN~~

- **702 Targets.** In addition to the explanation of target above, in the context of Section 702 the term “target” is generally used to refer to the act of intentionally directing intelligence collection at a particular person, a group, or organization. For example, the statutory provisions of Section 702 state that the Government “may not *intentionally target any person* known at the time of the acquisition to be located in the United States” (emphasis added), among other express limitations. Under Section 702, the Foreign Intelligence Surveillance Court (FISC) approves Certifications as opposed to individualized orders. Thus, the number of 702 “targets” reflects an estimate of the number of known users of particular facilities (sometimes referred to as selectors) subject to intelligence collection under those Certifications. This estimate is based on the information readily available to the Intelligence Community to identify unique targets – users, whose identity may be unknown, but who are reasonably believed to use the particular facility from outside the United States and who are reasonably believed to be non-United States persons. For example, foreign intelligence targets often communicate using several different email accounts. Unless the Intelligence Community has information that multiple email accounts are used by the same target, each of those accounts would be counted separately in these figures. On the other hand, if the Intelligence Community is aware that the accounts are all used by the same target, as defined above, they would be counted as one target.
- **Relationship of Orders to Targets.** In some cases, one order can by its terms affect multiple targets (as with Section 702). Alternatively, a target may be the subject of multiple orders, as noted below.
- **Amendments and Renewals.** The FISC may amend an order one or more times after it has been issued. For example, an order may be amended to add a newly discovered account used by the target. To avoid redundant counting, these statistics do not count such amendments separately. Moreover, some orders may be renewed multiple times during the calendar year (for example, the FISA statute provides that a Section 704 FISA Order against a U.S. person target may last no longer than 90 days but permits the order to be renewed). The statistics count each such renewal as a separate order.

#### **Title V of FISA (Business Records).**

We are reporting information about the Government’s use of the FISA Business Records provision (Title V) separately because this authority has been used in two distinct ways – collection of business records to obtain information about a specific subject and collection of business records in bulk. Accordingly, in the interest of transparency, we have decided to clarify the extent to which individuals are affected by each use. In addition, instead of reporting on the number of Business Record orders, the government is reporting on the number of *applications* submitted to the Foreign Intelligence Surveillance Court because the FISC may issue several orders to different recipients based upon a particular application.

~~TOP SECRET//NOFORN~~

Legal Authority	Annual Number of Applications	Estimated Number Affected
FISA Business Records (Title V of FISA)	178	172: The number of individuals, entities, or foreign powers subject to a business records application to obtain information about a specific subject
		423: The number of selectors approved to be queried under the NSA telephony metadata program
		248: The number of known or presumed U.S. persons who were the subject of queries of information collected in bulk or who were subject to a business records application.

### National Security Letters.

Finally, we are reporting information on the Government's use of National Security Letters (NSLs). On April 30, 2014, the Department of Justice released its Annual Foreign Intelligence Surveillance Act Report to Congress. That report, which is [available here](#) reports on the number of requests made for certain information concerning different United States persons pursuant to NSL authorities during calendar year 2013. In addition to those figures, today we are reporting (1) the total number of NSLs issued for all persons, and (2) the total number of requests for information contained within those NSLs. For example, one NSL seeking subscriber information from one provider may identify three e-mail addresses, all of which are relevant to the same pending investigation and each is considered a "request."

We are reporting the annual number of requests rather than "targets" for multiple reasons. First, the FBI's systems are configured to comply with Congressional reporting requirements, which do not require the FBI to track the number of individuals or organizations that are the subject of an NSL. Even if the FBI systems were configured differently, it would still be difficult to identify the number of specific individuals or organizations that are the subjects of NSLs. One reason for this is that the subscriber information returned to the FBI in response to an NSL may identify, for example, one subscriber for three accounts or it may identify different subscribers for each account. In some cases this occurs because the identification information provided by the subscriber to the provider may not be true. For example, a subscriber may use a fictitious name or alias when creating the account. Thus, in many instances, the FBI never identifies the actual subscriber of a facility. In other cases this occurs because individual

~~TOP SECRET//NOFORN~~

subscribers may identify themselves differently for each account, e.g., inclusion of middle name, middle initial, etc., when creating an account.

We also note that the actual number of individuals or organizations that are the subject of an NSL is different than the number of NSL requests. The FBI often issues NSLs under different legal authorities, e.g., 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709, for the same individual or organization. The FBI may also serve multiple NSLs for an individual for multiple facilities, e.g., multiple e-mail accounts, landline telephone numbers, cellular phone numbers, etc. The number of requests, consequently, is significantly larger than the number of individuals or organizations that are the subjects of the NSLs.

<b>Legal Authority</b>	<b>Annual Number of NSLs Issued</b>	<b>Annual Number of Requests for Information</b>
National Security Letters issued pursuant to 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709	19,212	38,832

This information will be available at the website of the Office of the Director of National Intelligence (ODNI); and ODNI's public website dedicated to fostering greater public visibility into the intelligence activities of the Government, [ICOntheRecord.tumblr.com](http://ICOntheRecord.tumblr.com).

~~TOP SECRET//NOFORN~~

# **EXHIBIT H**



U.S. Department of Justice  
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

The Honorable Harry Reid  
Majority Leader  
United States Senate  
Washington, DC 20510

APR 30 2013

Dear Mr. Leader:

This report is submitted pursuant to sections 107 and 502 of the Foreign Intelligence Surveillance Act of 1978 (the "Act"), as amended, 50 U.S.C. § 1801 *et seq.*, and section 118 of the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2006). In accordance with those provisions, this report provides information regarding all applications made by the Government during calendar year 2012 for authority to conduct electronic surveillance for foreign intelligence purposes under the Act, all applications made by the Government during calendar year 2012 for access to certain business records (including the production of tangible things) for foreign intelligence purposes, and certain requests made by the Federal Bureau of Investigation pursuant to national security letter authorities. In addition, while not required to do so by statute, the Government is providing information concerning the number of applications made during calendar year 2012 for authority to conduct physical searches for foreign intelligence purposes.

**Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2012 (section 107 of the Act, 50 U.S.C. § 1807)**

During calendar year 2012, the Government made 1,856 applications to the Foreign Intelligence Surveillance Court (the "FISC") for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. The 1,856 applications include applications made solely for electronic surveillance, applications made solely for physical search, and combined applications requesting authority for electronic surveillance and physical search. Of these, 1,789 applications included requests for authority to conduct electronic surveillance.

Of these 1,789 applications, one was withdrawn by the Government. The FISC did not deny any applications in whole or in part. The FISC made modifications to the proposed orders

The Honorable Harry Reid

Page 2

in 40 applications.<sup>1</sup> Thus, the FISC approved collection activity in a total of 1,788 of the applications that included requests for authority to conduct electronic surveillance.

**Applications for Access to Certain Business Records (Including the Production of Tangible Things) Made During Calendar Year 2012** (section 502 of the Act, 50 U.S.C. § 1862(c)(1))

During calendar year 2012, the Government made 212 applications to the FISC for access to certain business records (including the production of tangible things) for foreign intelligence purposes. The FISC did not deny, in whole or in part, any such application filed by the Government during calendar year 2012. The FISC made modifications to 200 proposed orders in applications for access to business records.

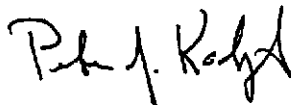
**Requests Made for Certain Information Concerning Different United States Persons Pursuant to National Security Letter Authorities During Calendar Year 2012** (USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2006))

Pursuant to Section 118 of the USA PATRIOT Improvement and Reauthorization Act, Pub. L. 109-177 (2006), the Department of Justice provides Congress with annual reports regarding requests made by the Federal Bureau of Investigation (FBI) pursuant to the National Security Letter (NSL) authorities provided in 12 U.S.C. § 3414, 15 U.S.C. § 1681u, 15 U.S.C. § 1681v, 18 U.S.C. § 2709, and 50 U.S.C. § 436.

In 2012, the FBI made 15,229 NSL requests (excluding requests for subscriber information only) for information concerning United States persons. These sought information pertaining to 6,223 different United States persons.

We hope that this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,



Peter J. Kadzik  
Principal Deputy Assistant Attorney General

---

<sup>1</sup> The FISC modified one order for an application made in a prior reporting period during the current reporting period.





**U.S. Department of Justice**

Office of Legislative Affairs

---

Office of the Assistant Attorney General

*Washington, D.C. 20530*

April 30, 2014

The Honorable Harry Reid  
Majority Leader  
United States Senate  
Washington, DC 20510

Dear Senator Reid:

This report is submitted pursuant to sections 107 and 502 of the Foreign Intelligence Surveillance Act of 1978 (the "Act"), as amended, 50 U.S.C. § 1801 *et seq.*, and section 118 of USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2006). In accordance with those provisions, this report provides information regarding all applications made by the Government during calendar year 2013 for authority to conduct electronic surveillance for foreign intelligence purposes under the Act, all applications made by the Government during calendar year 2013 for access to certain business records (including the production of tangible things) for foreign intelligence purposes, and certain requests made by the Federal Bureau of Investigation pursuant to national security letter authorities. In addition, while not required to do so by statute, the Government is providing information concerning the number of applications made during calendar year 2013 for authority to conduct physical searches for foreign intelligence purposes.

**Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2013** (section 107 of the Act, 50 U.S.C. § 1807)

During calendar year 2013, the Government made 1,655 applications to the Foreign Intelligence Surveillance Court (hereinafter "FISC") for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. The 1,655 applications include applications made solely for electronic surveillance, applications made solely for physical search, and combined applications requesting authority for electronic surveillance and physical search. Of these, 1,588 applications included requests for authority to conduct electronic surveillance.

None of these 1,588 applications were withdrawn by the Government. The FISC did not deny any applications in whole, or in part. The FISC made modifications to the proposed orders

The Honorable Harry Reid

Page 2

in 34 applications.<sup>1</sup> Thus, the FISC approved collection activity in a total of 1,588 of the applications that included requests for authority to conduct electronic surveillance.

**Applications for Access to Certain Business Records (Including the Production of Tangible Things) Made During Calendar Year 2013** (section 502 of the Act, 50 U.S.C. § 1862(c)(1))

During calendar year 2013, the Government made 178 applications to the FISC for access to certain business records (including the production of tangible things) for foreign intelligence purposes. The FISC did not deny, in whole or in part, any such application filed by the Government during calendar year 2013. The FISC made modifications to 141 proposed orders in applications for access to business records.

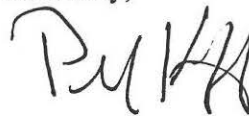
**Requests Made for Certain Information Concerning Different United States Persons Pursuant to National Security Letter Authorities During Calendar Year 2013** (USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2006))

Pursuant to Section 118 of the USA PATRIOT Improvement and Reauthorization Act, Pub. L. 109-177 (2006), the Department of Justice provides Congress with annual reports regarding requests made by the Federal Bureau of Investigation (FBI) pursuant to the National Security Letter (NSL) authorities provided in 12 U.S.C. § 3414, 15 U.S.C. § 1681u, 15 U.S.C. § 1681v, 18 U.S.C. § 2709, and 50 U.S.C. § 436.

In 2013, the FBI made 14,219 NSL requests (excluding requests for subscriber information only) for information concerning United States persons. These sought information pertaining to 5,334 different United States persons.<sup>2</sup>

We hope that this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,



Peter J. Kadzik

Principal Deputy Assistant Attorney General

---

<sup>1</sup> In addition to the 34 orders modified with respect to applications made during the reporting period, the FISC modified two orders for applications made in a prior reporting period during the current reporting period.

<sup>2</sup> In the course of compiling its National Security Letter statistics, the FBI may over-report the number of United States persons about whom it obtained information using National Security Letters. For example, NSLs that are issued concerning the same U.S. person and that include different spellings of the U.S. person's name would be counted as separate U.S. persons, and NSLs issued under two different types of NSL authorities concerning the same U.S. person would be counted as two U.S. persons. This statement also applies to previously reported annual U.S. person numbers.

**EXHIBIT I**

## REQUESTS FOR INFORMATION UNDER THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

*The Federal Bureau of Investigation may issue a national security letter to request, and a provider may disclose, only the four types of information—name, address, length of service, and local and long distance toll billing records—listed in 18 U.S.C. § 2709(b)(1).*

*The term “local and long distance toll billing records” in section 2709(b)(1) extends to records that could be used to assess a charge for outgoing or incoming calls, whether or not the records are used for that purpose, and whether they are linked to a particular account or kept in aggregate form.*

*Before issuance of a national security letter, a provider may not tell the FBI whether that provider serves a particular customer or telephone number, unless the FBI is asking only whether the number is assigned, or belongs, to that provider.*

November 5, 2008

### MEMORANDUM OPINION FOR THE GENERAL COUNSEL FEDERAL BUREAU OF INVESTIGATION

You have asked whether, under the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (“ECPA”), codified as amended at 18 U.S.C. § 2709 (2000 & West Supp. 2008), the Federal Bureau of Investigation (“FBI”) may obtain certain types of information from communications providers. *See* Memorandum for Steven G. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel, from Valerie Caproni, General Counsel, Federal Bureau of Investigation, *Re: Electronic Communications Privacy Act* (Aug. 28, 2007) (“FBI Memorandum”). Section 2709(b)(1) of ECPA enables the FBI to “request the name, address, length of service, and local and long distance toll billing records” of a subscriber, if that information may be “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.” The provider “shall comply” with such a request. *See id.* § 2709(a). In most other circumstances, ECPA prohibits the disclosure of a “record or other information pertaining to a subscriber to or customer of” a communications service. *See* 18 U.S.C.A. § 2702(a)(3).

In response to your specific questions, we conclude: (i) the FBI may issue a national security letter (“NSL”) to request, and a provider may disclose, only the four types of information—name, address, length of service, and local and long distance toll billing records—listed in section 2709(b)(1); (ii) the term “local and long distance toll billing records” in section 2709(b)(1) extends to records that could be used to assess a charge for outgoing or incoming calls, whether or not the records are used for that purpose, and whether they are linked to a particular account or kept in aggregate form; and (iii) before issuance of an NSL, a provider may not tell the FBI whether that provider serves a particular customer or telephone number, unless the FBI is asking only whether the number is assigned, or belongs, to that provider.<sup>1</sup>

---

<sup>1</sup> We solicited and received the views of the National Security Division and the Criminal Division on these questions.

*Opinions of the Office of Legal Counsel in Volume 32*

I.

Under 18 U.S.C. § 2709(a), a wire or electronic communications service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

Section 2709(b)(1), in turn, enables the Director or his designee to

request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.

You have asked whether the four types of information listed in subsection (b)(1)—the subscriber’s name, address, length of service, and local and long distance toll billing records—are exhaustive or merely illustrative of the information that the FBI may request and a provider may turn over. We conclude that the list in section 2709(b)(1) is exhaustive.<sup>2</sup>

A.

We begin with the text of the statute. *Limtiaco v. Camacho*, 127 S. Ct. 1413, 1418 (2007). Section 2709(b) authorizes the FBI to request from a provider “the name, address, length of service, and local and long distance toll billing records of a person or entity.” By its express terms, subsection (a), which specifies the information that the provider is to disclose, reaches no further than the information that the FBI may request under subsection (b): subsection (a) requires a provider to comply with a request for “subscriber information and toll billing records information” made by the FBI “*under subsection (b)*.” 18 U.S.C. § 2709(a) (emphasis added). Subsection (b) specifies the items for which the FBI may ask, and there is no indication that the list of items is illustrative. *Cf. Burgess v. United States*, 128 S. Ct. 1572, 1578 n.3 (2008) (examples where the word “includes” may enlarge the meaning of a definition beyond the terms in the list). The list—the name, address, length of service, and local and long distance toll billing records of a person or entity, *see id.* § 2709(b)(1)—thus sets the limits of what the FBI may request under section 2709, as well as what the provider may disclose under that provision. The text of subsection (b) forecloses an interpretation that would add other types of information

---

<sup>2</sup> Although the same issue could arise under section 2709(b)(2), we refer to section 2709(b)(1) for convenience, because your question about “toll billing records,” to which we turn below, relates only to section 2709(b)(1).

*Requests for Information under the Electronic Communications Privacy Act*

to the excepted categories. *See Swierkiewicz v. Sorema N.A.*, 534 U.S. 506, 513 (2002) (applying the canon of *expressio unius est exclusio alterius*).<sup>3</sup>

ECPA’s structure reinforces this conclusion. Section 2709 is an exception to the background rule of privacy established by 18 U.S.C. § 2702(a), which generally bars a provider from giving the Government a record or other information pertaining to a subscriber or customer. Here, the exceptions listed in section 2709(b)(1) specify some types of information—a subscriber’s name, address, length of service, and billing records—and not others. Other exceptions to the rule of privacy appear in section 2702(b), dealing with voluntary disclosures, and in section 2703, dealing with disclosures in response to subpoenas or warrants. We would not infer additional exceptions. *See* 2A Norman J. Singer, *Statutes and Statutory Construction* § 47.11, at 250-51 (6th ed. 2000) (“Where there is an express exception, it comprises the only limitation on the operation of the statute and no other exceptions will be implied. . . . [W]here a general provision in a statute has certain limited exceptions, all doubts should be resolved in favor of the general provision rather than the exceptions.”).<sup>4</sup>

The FBI Memorandum suggests that, under basic principles of interpretation, the general term “subscriber information” should be construed in light of specific examples in the statute. FBI Memorandum at 3-4. According to the FBI Memorandum, the term “subscriber information” in subsection (a) should encompass all information similar to the types specified in subsection (b), so that a provider could turn over, for example, a subscriber’s date of birth or social security number. Under the widely employed canon of statutory construction known as “*ejusdem generis*,” “where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words.” *Circuit City Stores v. Adams*, 532 U.S. 105, 114-15 (2001) (internal quotation marks and citation omitted); *see also Vanderbrook v. Unitrin*

---

<sup>3</sup> Subsection (a) also refers to “electronic communication transactional records” requested under subsection (b). In its current form, however, subsection (b) does not include this term. As originally enacted, subsection (b) did not specify the items of information that the FBI could request, but simply provided the means by which the FBI could ask for “any such information and records” as were described in subsection (a). Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1867 (1986). When Congress in 1993 added to subsection (b) the specification of “name, address, length of service, and toll billing records,” it did not include “electronic communication transactional records” in that list. Pub. L. No. 103-142, 107 Stat. 1491 (1993). Nevertheless, the reference to “electronic communication transactional records” in subsection (a), along with the absence of the phrase in subsection (b), does not undermine the conclusion that the categories of information listed in subsection (b) are exclusive. As the committee report on the original enactment explained, the language about “electronic communication transactional records” gives the FBI “the necessary authority [to issue NSLs] with regard to subscriber information and toll billing information with respect to electronic communication services other than ordinary telephone service.” S. Rep. No. 99-541, at 44 (1986) (emphasis added). While clarifying that NSLs can extend to other types of services, therefore, the language reaches only those categories of information parallel to subscriber information and toll billing records for ordinary telephone service.

<sup>4</sup> The conclusions in this memorandum apply only to disclosures under section 2709. We do not address other statutory provisions under which law enforcement officers may get information pertaining to electronic communications. *See, e.g.*, 18 U.S.C. § 2702(b)(8), (c)(4) (West Supp. 2008) (authorizing disclosure of communications and customer records to governmental entities if the provider reasonably “believes that an emergency” involving “danger of death or serious physical injury to any person” justifies disclosure of the information); *id.* § 2703(a) (authorizing disclosure to a governmental entity of “the contents of a wire or electronic communication” pursuant to a warrant).

*Opinions of the Office of Legal Counsel in Volume 32*

*Preferred Ins. Co.*, 495 F.3d 191, 219 (5th Cir. 2007) (noting that the *ejusdem generis* canon “is used to interpret general terms (e.g., ‘and the like’) following a list of specific terms”). The canon thus allows a list of specific terms to define and limit an otherwise ambiguous term within the same list. See, e.g., 2A Norman J. Singer, *Statutes and Statutory Construction* § 47.17, at 188 (5th ed. 1992). The FBI Memorandum, however, would rely on this canon to draw the reverse inference, by expanding the meaning of a general term (“subscriber information”) that appears outside the list of terms in section 2709(b) and in a separate subsection of the statute. Even if the text of section 2709(a) were unclear, the canon of *ejusdem generis* would offer little support for the argument that subsection (a) should be interpreted more broadly than subsection (b). In any event, because the text of subsection (a) shows that a provider is to supply only information requested under subsection (b), the canon of *ejusdem generis* does not apply. See, e.g., *Tourdot v. Rockford Health Plans, Inc.*, 439 F.3d 351, 354 (7th Cir. 2006) (noting that the canon of *ejusdem generis* applies only where a statutory term is ambiguous, that it may not be used “both to create and to resolve [a statutory] ambiguity,” and that it “may not be used to defeat the obvious purpose or plain meaning of the text”).

**B.**

The FBI Memorandum also relies upon the legislative history of ECPA’s 1993 amendments to argue that, using NSLs, the FBI may seek and providers may disclose—as “subscriber information”—“any information kept by the communications service provider for its own business purposes that identifies the subscriber,” not just the types of information listed in section 2709(b). FBI Memorandum at 5. In our view, the language of the provision is straightforward, and “[g]iven [a] straightforward statutory command, there is no reason to resort to legislative history.” *United States v. Gonzales*, 520 U.S. 1, 6 (1997). In any event, we believe that the legislative history accords with our conclusion.

In a passage that the FBI Memorandum cites, the House Judiciary Committee Report for the 1993 amendments stated that “[t]he Committee intends . . . that the authority to obtain subscriber information . . . under section 2709 does not require communications service providers to create records which they do not maintain in the ordinary course of business.” H.R. Rep. No. 103-46, at 3 (1993), *reprinted in* 1993 U.S.C.C.A.N. 1913, 1915. While the legislative history of ECPA therefore suggests that the statute does not require a provider to “create” new records, it does not follow that the statute would authorize the FBI to seek, or the provider to disclose, any records simply because the provider has already created them in the ordinary course of business. The universe of records subject to an NSL is still restricted to the types listed in the statute.<sup>5</sup>

Indeed, the 1993 amendments clarified and underscored the limitations on the scope of “subscriber information.” As the House Judiciary Committee Report explained, “[i]nstead of ‘subscriber information,’ the amendment here uses *more specific* terms: ‘name, address, length of service.’” H.R. Rep. No. 103-46, at 3, *reprinted in* 1993 U.S.C.C.A.N. at 1915 (emphasis added). More generally, the Report set the context of the amendments by declaring that “the

---

<sup>5</sup> We do not address whether the FBI must purge its files of any additional information given to it by communications providers.

*Requests for Information under the Electronic Communications Privacy Act*

national security letter is an extraordinary device” and that “[n]ew applications [for its use] are disfavored.” *Id.* at 3, *reprinted in* 1993 U.S.C.C.A.N. at 1914-15. Where Congress enlarged the FBI’s authority in the 1993 amendments, it placed careful limits on the new authority. It rejected one FBI proposal as “too broad” and substituted a narrower provision. *See id.* at 2, *reprinted in* 1993 U.S.C.C.A.N. at 1914. The Report, therefore, reinforces our construction of the text.

## II.

Next, you have asked whether, under section 2709, the term “local and long distance toll billing records” includes records of incoming and outgoing calls upon which a charge could be assessed, whether or not a provider actually assesses a charge, and whether or not a provider maintains such records as aggregate data (as opposed to subscriber-specific data). We believe that the term includes records of individual calls identifying the telephone numbers called from a particular telephone number or attributed to a particular account, if maintained in the normal course of a provider’s business, whether or not the provider charges for each such call. In our view, moreover, section 2709 encompasses call records stored in aggregate form, even if they are not organized by customer accounts, provided that, as explained below, an NSL for such information is not unreasonably burdensome.

### A.

Section 2709(a) requires a provider, in response to an NSL, to supply “subscriber information and toll billing records information.” As we explained in part I, section 2709(b) specifies the “subscriber information and toll billing records information” that an NSL may demand and a provider may supply. This information consists of “the name, address, length of service, and local and long distance toll billing records of a person or entity.” In addition to “subscriber information,” therefore, an NSL may demand, and a provider must turn over, “toll billing records information,” consisting of “local and long distance toll billing records.”

The “billing records” to which section 2709 refers could denote either records that are actually used for billing or records that could be used for that purpose. In the abstract, either meaning could be a natural use of language. For example, the phrase “running shoes” could mean either shoes actually used for running or those of a type making them suitable for that purpose, even if the owner only walks. We believe that the phrase “local and long distance toll billing records” covers records—including the caller’s number, the number dialed, and the duration of the call—that are suitable for billing, whether or not the provider imposes a per call “toll.”

As originally enacted, section 2709(b) provided that the FBI could use NSLs to seek “toll billing records.” *See* 100 Stat. at 1867. In 1996, Congress amended the provision to read “local and long distance toll billing records.” *See* Intelligence Authorization Act for Fiscal Year 1997, Pub. L. No. 104-293, § 601, 110 Stat. 3461, 3469 (1996). The amendments clarified that billing records for local service, as specified in section 2709(b)(1), could be a type of “toll billing records information” that section 2709(a) directs a provider to turn over in response to an NSL. The reference in section 2709(b)(1) to billing records for “local” service, as a type of “toll billing records information” within section 2709(a), makes sense only if it encompasses records that are



*Opinions of the Office of Legal Counsel in Volume 32*

not actually used for billing customers, but are of a type that could be put to that use, because “local” service has traditionally been understood to be service for which the provider does not impose a per call “toll.”

The terms “local” and “long distance toll” are well established terms in the communications industry. *See, e.g., N.C. Utils. Comm’n v. FCC*, 552 F.2d 1036, 1045 (4th Cir. 1977) (distinguishing local service from “‘toll,’ or long distance, service” and suggesting both are “term[s] of art”). Traditionally, local service has been identified and defined by the absence of per call charges, or “tolls.” *See Newton’s Telecom Dictionary* 488 (20th ed. 2004) (defining “local call” as one that “may or may not cost money. In many parts of the United States, the phone company bills its local service as a ‘flat’ monthly fee.”). By contrast, long distance service has been defined by the use of per call “toll” charges. *See id.* at 839 (defining “toll call” as “[a] long distance call”); *see also Webster’s Third New International Dictionary* 2405 (1993) (defining “toll” as “a charge for a long-distance telephone call”).

Congress has distinguished between “local” and “long distance toll” calls on this basis for as long as the federal Government has regulated the telecommunications industry. In section 3 of the Communications Act of 1934, for example, Congress defined the term “telephone toll service” as “telephone service between stations in different exchange areas *for which there is made a separate charge* not included in contracts with subscribers for exchange service.” Act of June 19, 1934, c. 652, § 3, 48 Stat. 1064, 1066, codified at 47 U.S.C. § 153(s) (1934) (emphasis added). Congress separately defined “telephone exchange service,” otherwise known as “local” service, as “service within a telephone exchange, or . . . within the same exchange area . . . and *which is covered by the exchange service charge.*” 48 Stat. at 1066, codified at 47 U.S.C. § 153(r) (1934) (emphasis added). As the Federal Communications Commission explained in its rule implementing the AT&T consent decree, the definitions in the Communications Act “rel[y] primarily upon the non-toll or toll nature of a call to determine whether the call is a [local] or [long-distance] call.” *See* Memorandum Opinion, Order and Authorization, FCC 83-566, 96 F.C.C.2d 18, ¶ 17 n.24 (Dec. 23, 1983); *see also OfficeMax, Inc. v. United States*, 428 F.3d 583, 596 (6th Cir. 2005) (explaining that before the divestiture of AT&T, all long distance calls were subject to tolls, which varied according to the duration of the call and the distance between the callers); Howard A. Shelanski, *Adjusting Regulation to Competition: Toward a New Model for U.S. Telecommunications Policy*, 24 *Yale J. on Reg.* 55, 59-60 (2007) (noting that before divestiture of its local assets, “AT&T charged flat monthly fees for local service, [but] it charged by the minute for long-distance service, and the [Federal Communications Commission] allowed AT&T to set long-distance rates well above cost for the purpose—at first implicit and later expressly stated—of providing profits AT&T could use to cross-subsidize local rates in support of universal service policies”).

Even the tax code draws the distinction between “local” and “toll” calls. For example, the Excise Tax Reduction Act of 1965, Pub. L. No. 89-44, 79 Stat. 136, 145 (1965) (“ETRA”), amended the Internal Revenue Code to impose a three percent excise tax on, among other things, “local telephone services.” *See* 26 U.S.C. §§ 4251(b)(1)(A), 4252(a) (2000). Excluded from the definition of the term “local telephone services” was any “toll telephone service,” as defined in section 4252(b). *See, e.g., Reese Bros., Inc. v. United States*, 447 F.3d 229, 233 (3d Cir. 2006); *Western Elec. Co. v. United States*, 564 F.2d 53, 55 (Ct. Cl. 1977). “Toll telephone service”

*Requests for Information under the Electronic Communications Privacy Act*

means, in relevant part, a “telephonic quality communication for which . . . there is a toll charge which varies in amount with the distance and elapsed transmission time of each individual communication.” 26 U.S.C. § 4252(b)(1).<sup>6</sup>

In view of this background, when Congress inserted the words “local and long distance” before “toll billing records” in section 2709(b)(1), it was not limiting ECPA to those local calls for which a provider imposes a per call “toll.” We presume that Congress understood the well established distinction between “local” and “long distance toll” calls and knew that “local” service was frequently *defined* by the absence of a per call charge. See *Standard Oil Co. v. United States*, 221 U.S. 1, 59 (1911) (“[W]here words are employed in a statute which had at the time a well-known meaning at common law *or in the law of this country* they are presumed to have been used in that sense.”) (emphasis added); Felix Frankfurter, *Some Reflections on the Reading of Statutes*, 47 Colum. L. Rev. 527, 537 (1947) (“[I]f a word is obviously transplanted from another legal source, whether the common law or other legislation, it brings the old soil with it.”). Therefore, the reference to “billing records” for “local” service in section 2709(b)(1), as a type of “toll billing records information” that section 2709(a) requires a provider to turn over, is best read to cover records that *could* be used for per call billing, not only those that actually are used for that purpose.

When Congress enacted the 1996 amendments, it was well known that providers of telephone service might keep records of local calls from or attributable to particular numbers, even if they did not assess per call charges. Providers had long used pen registers, for example, to record all telephone numbers dialed from particular telephones, whether the calls were local or long distance. See, e.g., *Smith v. Maryland*, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) (emphasizing that the Court’s conclusion hinges on the fact “that pen registers are regularly used for recording local calls”); *Hodge v. Mountain States Tel. & Tel. Co.*, 555 F.2d 254, 266 (9th Cir. 1977) (Hufstedler, J., concurring) (emphasizing that pen registers collect records of local calls); *In the Matter of Grand Jury Subpoenas to Southwestern Bell Mobile Systems, Inc.*, 894 F. Supp. 355, 358 (W.D. Mo. 1995) (“*Southwestern Bell*”) (holding the term “toll billing records” means ““billing records and telephone toll records (including the record of long distance numbers and message unit detailing information)””) (quoting H.R. 99-647, 99th Cong., 2d Sess., 69 (1986)); *People v. Guerra*, 478 N.E.2d 1319, 1321 (N.Y. 1985) (noting pen registers “provide a list of all numbers dialed, both local and long distance or toll calls,” and that such information is included in phone companies’ billing records).<sup>7</sup> The reference to “toll billing records” covers this type of information.

---

<sup>6</sup> Congress acknowledged that telephone companies might choose not to impose per call charges for some “toll telephone service.” For example, ETRA defined “toll telephone service” as, among other things, “a [non-local] service which entitles the subscriber, upon payment of a periodic charge (determined as a *flat amount* or upon the basis of total elapsed transmission time), to the privilege of an unlimited number of telephonic communications.” 79 Stat. at 146 (emphasis added). See also *Reese Bros.*, 447 F.3d at 233-34 (noting that before 1984, AT&T offered a type of “long-distance service[]” known as “Wide Area Telephone Service,” the bills for which “were based on a flat rate for unlimited calls”). As explained below, see *infra* p. 8, ECPA’s use of the term “long distance toll billing records” encompasses records of long distance calls, even if a telephone company uses “flat rate” (as opposed to per call) billing for long distance service.

<sup>7</sup> See also *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 174-75 (1977) (noting that phone companies use pen registers “for the purposes of checking billing operations,” among other things); *United States v. Clegg*, 509 F.2d 605, 608 & n.2 (5th Cir. 1975) (describing the “TTS 176” device, which “monitors the line to which it is

*Opinions of the Office of Legal Counsel in Volume 32*

The single occurrence of the words “billing records” in section 2709 applies to both “local” and “long distance toll” services. Because in the case of local service the phrase “billing records” covers records that could be used for billing, we would accord it the same meaning when the phrase applies to long distance service. Consequently, even if a provider does not impose per call charges for long distance service, we believe that the provider’s records, if suitable for billing, are subject to disclosure under an NSL.<sup>8</sup>

The interpretation that “billing records” extends to records usable for billing, even if not actually used for that purpose, is supported by the limited judicial authority on the point and by the legislative history of the 1996 amendments. Before 1996, 18 U.S.C. § 2703 authorized law enforcement officials to subpoena a subscriber’s “telephone toll billing records” during the course of an official investigation. Similarly, 18 U.S.C. § 2709 enabled the Director of the FBI to use an NSL to obtain a subscriber’s “toll billing records” during the course of an authorized foreign counterintelligence investigation. The United States District Court for the Western District of Missouri held that the term “telephone toll billing records,” under section 2703, included

any record (except a record pertaining to the content of a conversation) maintained by an electronic communication service provider identifying the telephone numbers called from a particular telephone number or attributed to a particular account for which a communication service provider might charge a service fee. ‘Telephone toll billing records’ covers all records maintained of individual calls made from a particular telephone number or attributed to it that

---

attached and produces a paper tape record of the time and date of all outgoing telephone calls, local and long distance, complete and incomplete,” and which phone companies use “to show both that its billing procedures were bypassed and that completed calls were made”); *United States v. Fithian*, 452 F.2d 505, 506 (9th Cir. 1971) (noting that a phone company’s “business records necessarily must contain” the “records of calls from [a subscriber’s] residence”); *cf. Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co.*, 593 F.2d 1030, 1046 n.49 (D.C. Cir. 1978) (noting that “a telephone subscriber has no Fourth Amendment interest in local call records obtained by means of a pen register installed without his knowledge”).

<sup>8</sup> The use of per call charges may be less prevalent today than in 1996, when Congress amended ECPA. Cellular phone customers typically do not incur per call charges for either local or long distance service, and cellular phone use has multiplied since 1996. *See Statistical Abstract of the United States* at 720 (U.S. Census Bureau, 2007) (noting that there were fewer than 34 million cellular phone subscribers in the United States in 1995, whereas there were almost 208 million in 2005 (the most recent year for which statistics are available)). Partly in response to the pricing strategies employed by cellular phone companies, other telecommunications providers have shifted to “flat rate billing.” *See, e.g., Kathleen Q. Abernathy, Preserving Universal Service in the Age of IP*, 3 J. Telecomm. & High Tech. L. 409, 412 (2005) (describing “the increasing prevalence of bundled service plans” as an “important trend” in the telecommunications industry). As then-FCC Commissioner Abernathy explained, “For years, wireless carriers have offered buckets of any-distance minutes at flat rates, and now wireline carriers are offering packages that include local and long distance for a single price. In addition, many carriers offer business customers bundles that include local and long distance voice services, Internet access, and customer premises equipment.” *Id.* (footnote omitted). The provision of telephone service over Internet connections—as opposed to traditional wireline or wireless technologies—has further contributed to the decline in per call billing. *See id.*; *see also* Steven C. Judge, *VoIP: A Proposal for a Regulatory Scheme*, 12 Syracuse Sci. & Tech. L. Rep. 77 (2005) (“[I]nstead of paying a per minute charge for long distance calls, many [voice over internet protocol, or “VoIP”] providers provide a flat rate that includes both local- and long-distance calling.”). However providers may charge for such services, we conclude that ECPA covers any call record in a provider’s custody or possession that is suitable for billing.

*Requests for Information under the Electronic Communications Privacy Act*

are *or could be* the subject of a particularized charge depending on the billing plan offered by the provider and accepted by the customer. *In other words, a telephone toll billing record is broad enough to cover all records of calls from or attributed to a particular number, regardless of whether, in fact, a separate charge is assessed for each call.*

*Southwestern Bell*, 894 F. Supp. at 359 (emphasis added). The court relied upon ECPA’s legislative history, which indicates that “toll billing records consist of information maintained by a wire or electronic communication service provider identifying the telephone numbers called from a particular phone or attributable to a particular account for which a communication service provider *might* charge a service fee.” *Id.* at 358 (quoting 1993 U.S.C.C.A.N. at 1915). Accordingly, the court held that, even when a cellular phone subscriber had a monthly plan under which he did not pay a “toll” for any particular call, the record of every call he made, local or long distance, fell within the meaning of “telephone toll billing records” under section 2703.

In 1996, Congress amended section 2703, as well as section 2709, to ratify the decision in *Southwestern Bell*. See Intelligence Authorization Act for Fiscal Year 1997, Pub. L. No. 104-293, § 601, 110 Stat. 3461, 3469 (1996). The 1996 amendments inserted the words “local and long distance” before the words “toll billing records” in both section 2703 and section 2709. *Id.* The Senate Report explained that the amendments “make clear . . . that the phrase [‘toll billing records’] applies to both local and long distance telephone toll billing records” in accordance with the decision in *Southwestern Bell*. S. Rep. No. 104-258, at 22 (1996), *reprinted in* 1996 U.S.C.C.A.N. 3945, 3967. The committee quoted the court’s holding that a provider must disclose “records that contain information which was used *or could be used* to charge for telephone calls or services.” *Id.* (emphasis added).

We therefore conclude that the term “local and long distance toll billing records” extends to records of individual calls identifying the telephone numbers called from a particular telephone number or attributed to a particular account, whether or not the provider charges individually for each such call.<sup>9</sup>

## B.

Telecommunications providers generally maintain call data in one of two forms: call records linked to particular accounts (such as records of a given customer’s calls and associated charges), and aggregate records (such as records of all calls routed through a particular call center on a particular day). See, e.g., *Ameritech Corp. v. McCann*, 403 F.3d 908, 910 (7th Cir. 2005). The aggregate records are generally stored on “searchable media” that a carrier could cull to extract records of calls to or from a particular number. See *id.* The records culled in this way

---

<sup>9</sup> Whether the statute should be read to cover “local . . . billing records” or “local . . . toll billing records” would not affect our analysis. See S. Rep. No. 104-258, at 22 (1996), *reprinted in* 1996 U.S.C.C.A.N. 3945, 3967 (“This amendment is a clarification of the meaning of the phrase ‘telephone toll billing records’ as used in [sections] 2703 and 2709.”). In either case, the phrase is a more detailed formulation of “toll billing records” in section 2709(a). A provider can disclose information if it is a “toll” record of an incoming or outgoing call, as explained above. If the information is not such a “toll” record, the provider can disclose it only if it is “subscriber information”—the “name, address, and length of service” of the subscriber. See 18 U.S.C. § 2709(a), (b)(1).

*Opinions of the Office of Legal Counsel in Volume 32*

could be used to bill for the service to a particular number, although they are not typically used for this purpose.

Because section 2709 covers records of calls for which a carrier could impose charges—even if the carrier does not actually do so—it does not matter whether the provider maintains those records in the form of billing statements that reflect actual per call charges on customers' accounts. Under 18 U.S.C. § 2709(b)(1), an NSL may request “the name, address, length of service, and local and long distance toll billing records of a person or entity,” and the records of a subscriber's calls are “records of [that] person or entity,” even if the calls of a particular subscriber are dispersed among the aggregate records of all calls going through a call center. Responding to the NSL, a provider must turn over any “local and long distance toll billing records” in its “custody or possession.” 18 U.S.C. § 2709(a). Even if a provider maintains its call data in aggregate form, the billing records are in the provider's “custody or possession” and fall within section 2709. To comply with the NSL, therefore, the provider would have to extract the subscriber data from the aggregate records.

This conclusion is consistent with the Seventh Circuit's decision in *McCann*, which interpreted 18 U.S.C. § 2706 (2000). Under section 2706, governmental entities, state or federal, must compensate providers for complying with certain requests or demands for information other than NSLs, except when a request seeks “records or other information maintained by a communications common carrier that relate to telephone toll records” and that request does not present an undue burden. In *McCann*, the court held that certain aggregate call data did not constitute such “records or other information” within the exception, because the provider did not “maintain” the data as sought there. *See* 403 F.3d at 912 (characterizing the process of culling data as the “creat[ion]” of reports). The Department has questioned whether *McCann* was correctly decided. *See 18 U.S.C. § 2706 (ECPA) Cost Reimbursement Guidance*, U.S. Dep't of Justice Ad Hoc Technology Working Group, at 5 (May 25, 2005) (arguing that “there is a reasonably strong argument that *Ameritech Corp. v. McCann*'s interpretation of section 2706 is flawed”). Even if correct, *McCann*'s interpretation of section 2706 would not reach NSLs, which are issued under section 2709. The Seventh Circuit's decision turned exclusively on the meaning of “maintain” in section 2706(c)—a term that does not appear in section 2709, *compare id.* § 2709(a) (referring to “records in [a carrier's] custody or possession”)—and the court did not address the meaning of “telephone toll records,” let alone the meaning of “local and long distance toll billing records.”

As the FBI Memorandum notes, some providers have argued that culling records of individual calls from aggregate call data amounts to the “creation” of a new record, in contravention of *Southwestern Bell*, as well as the House report upon which that decision relied. *See* FBI Memorandum at 9. The *Southwestern Bell* court emphasized, however, that a carrier may be asked to turn over all call records in the carrier's custody, even if a particular customer does not choose a per call billing plan. *See* 894 F. Supp. at 359. To be sure, the FBI may not be able to force a communications provider to alter its business practices and, for example, create and maintain records of per call usage. *See id.* at 358-59 (quoting and relying upon H. Rep. No. 103-46, 1993 U.S.C.C.A.N. 1913, 1915, which provides that “the authority to obtain subscriber information and toll billing records under § 2709 does not require communication service providers to create records which they do not maintain in the ordinary course of business”).

*Requests for Information under the Electronic Communications Privacy Act*

But to the extent that a communications provider, in the ordinary course of business, collects information regarding the calls made to or from a particular account and could use that information for billing a customer, such information—however it is stored—falls within section 2709.

At the same time, the FBI may not use section 2709 to demand that a telecommunications provider cull data if the search would be unduly costly or burdensome. An NSL is, in effect, an administrative subpoena: it is an agency order requiring the production of specified information, issued as part of an investigation. We would read section 2709 in light of the principle that, as the Supreme Court has held, the Fourth Amendment “in no way leaves a [firm] defenseless against an unreasonably burdensome administrative subpoena requiring the production of documents.” *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984). An administrative subpoena must be “sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.” *Id.* (quoting *See v. City of Seattle*, 387 U.S. 541, 544 (1967)). In other contexts, ECPA deals with a possible undue burden by requiring the government to compensate the provider for the costs of the search. *See* 18 U.S.C. § 2706. Particularly because ECPA allows no such payment for complying with an NSL, we would construe section 2709 as not enabling the FBI to force a provider to cull data when it would be unduly costly or burdensome for the provider to do so. A provider would not have to comply with an unduly burdensome NSL.

Therefore, any call record that a communications provider keeps in the regular course of business and could use for billing a subscriber falls within the scope of section 2709. As in the case of administrative subpoenas, however, an NSL may not be unreasonably burdensome.<sup>10</sup>

### III.

Finally, you have asked whether a provider, in answer to an oral request before service of an NSL, may tell the FBI whether a particular account exists. This information would be confined to whether a provider serves a particular subscriber or a particular phone number. We believe that ECPA ordinarily bars providers from complying with such requests.

Section 2702(a)(3) states that “a provider of . . . electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity.” 18 U.S.C. § 2702(a)(3). That a subscriber receives services from a particular provider is “information pertaining to” the subscriber. Indeed, section 2709 lists the subscriber’s name among the types of “subscriber information” that an NSL can request. Therefore, when the FBI identifies a subscriber by name, section 2702(a)(3) forbids a provider from divulging the existence of that person’s or entity’s subscription with the provider.

Although the question is far closer, we do not believe that this conclusion changes if the FBI identifies a phone number, rather than a customer’s name, where the FBI is asking whether the number has been given to a subscriber. The phrase “record or other information pertaining to

---

<sup>10</sup> We express no view on what would constitute an unreasonably burdensome request.

*Opinions of the Office of Legal Counsel in Volume 32*

a subscriber” is broad. The ordinary meaning of “pertaining,” in this phrase, would reach information that “relate[s] to” or “concern[s]” the subscriber, *Black’s Law Dictionary* 1165 (7th ed. 1999), or has “some connection with or relation to” him, *Webster’s Third New International Dictionary* 1688 (1993). The fact of a provider’s service to a given number constitutes “information pertaining to a subscriber,” because it indicates that the provider serves “a subscriber” (or, in some cases, each of several subscribers) with that phone number. The information is associated with a particular subscriber, even if that subscriber’s name is unknown.

We do not believe that, for this analysis, it matters whether the information sought by the FBI has already been made public, unless the subscriber has given a consent broad enough to cover a response to the FBI’s request. An example of such consent would be the subscriber’s having a listed number. *See* 18 U.S.C. § 2702(c)(2). Without such consent, section 2702(a)(3), by its terms, bars a provider from supplying otherwise protected information, even if it has become public. Nor would it matter whether such information falls outside the category of “customer proprietary network information” under the Communications Act, so that its disclosure would not be unlawful under that statute. *See* 47 U.S.C. § 222(h) (2000). ECPA may forbid disclosure of particular information, even if the Communications Act does not.<sup>11</sup>

Nevertheless, if the FBI asks only whether a number is among those assigned, or belonging, to the provider and not whether the provider has given it to a subscriber, we do not believe that the inquiry seeks “information pertaining to a subscriber.” A provider’s confirmation that a number is assigned, or belongs, to it would not reveal whether the number is being used by a subscriber.

/s/

DANIEL L. KOFFSKY  
Deputy Assistant Attorney General

---

<sup>11</sup> A provider that does not serve a given individual or phone number would not appear to be revealing “information pertaining to a subscriber” by answering the FBI’s request in the negative. Nevertheless, once a provider has given this negative answer in one instance, a response of “no comment” in a later instance could have the effect of disclosing “information pertaining to a subscriber.” By entertaining the question at all, the provider would risk disclosing protected information.

**EXHIBIT J**





Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

DEC 23 2002

The Honorable Patrick J. Leahy  
Chairman  
Committee on the Judiciary  
United States Senate  
Washington, D.C. 20510

Dear Mr. Chairman:

Enclosed please find a response to your written question submitted to the Deputy Attorney General at the hearing before the Senate Judiciary Committee on May 8, 2002. We are providing a response to question 19 relating to the changes section 215 of the USA PATRIOT Act made to provisions of the Foreign Intelligence Surveillance Act (FISA). The Department is continuing to gather information to answer the remaining questions posed to the Deputy Attorney General and the Director of the Federal Bureau of Investigation, and we will forward those responses as soon as possible.

Please note that the response to question 19 requires the Department to provide information that is classified at the SECRET level. That classified information is being delivered to the Committee under separate cover and in accordance with the longstanding Executive branch practices on the sharing of operational intelligence information with Congress.

We appreciate your oversight interest in the Department's activities pursuant to the USA PATRIOT Act. We look forward to continuing to work with the Committee as the Department implements these important new tools for law enforcement in the fight against terrorism. If we can be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

Daniel J. Bryant  
Assistant Attorney General

Enclosure

cc: The Honorable Orrin G. Hatch  
Ranking Minority Member

**Questions Submitted by Chairman Leahy  
Senate Judiciary Committee Hearing on  
May 8, 2002**

*Questions for Director Mueller and Deputy Attorney General Thompson*

19. **Section 215 of the Patriot Act allows all FBI Special Agents in Charge to obtain court orders requiring the production of "any tangible things (including books, records, papers, documents, and other items)" in connection with terrorism investigations. There have been reports that this authority is being used to obtain records, without showing probable cause that a crime has been committed, from a library or bookstore about what books a person has signed out or purchased.**

**(a) Has the FBI, in fact, requested such records in any investigation of terrorism?**

**Answer:** Section 215 amended the business records authority found in Title V of the Foreign Intelligence Surveillance Act (FISA). Under the old language, the FISA Court would issue an order compelling the production of certain defined categories of business records upon a showing of relevance and "specific and articulable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power. The USA PATRIOT Act changed the standard to simple relevance and gives the FISA Court the authority to compel production in relation to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

The classified semi-annual report discussing the use of sections 1861-1863 of FISA for the period June 30, 2001 through December 31, 2001 was provided to the Intelligence and Judiciary committees of both houses of Congress on April 29, 2002. That report was provided under cover letter to each committee chairman. Although not specified in the statute, the Department's practice has been to submit the reports covering January 1 through June 30 of a given year, by the end of December of that year. The Department of Justice is currently preparing the semi-annual report covering the period January 1, 2002 through June 30, 2002.

The Department is able at this time to provide information pertaining to the implementation of section 215 of the USA PATRIOT Act from January 1, 2002 to the present (December 23, 2002). That information is classified at the SECRET level and, accordingly, is being delivered to the Committee under separate cover.

**(b) Can such an order be served on a public library to require the library to produce records about where a library patron has surfed on the Internet? Has such an order been sought by the Department or the FBI?**

**Answer:** Such an order could conceivably be served on a public library although it is

unlikely that public libraries maintain those types of records. If the FBI were authorized to obtain the information the more appropriate tool for requesting electronic communication transactional records would be a National Security Letter (NSL). NSLs can be served on Internet Service Providers to obtain information such as subscriber name, screen name or other on-line names, records identifying addresses of electronic mail sent to and from the account, records relating to merchandise orders/shipping information, and so on but not including message content and/or subject fields.

**(c) Do you think that library and bookstore patrons have a "reasonable expectation of privacy" in the titles of the books they have purchased from a bookstore or borrowed from a library?**

**Answer:** Any right of privacy possessed by library and bookstore patrons in such information is necessarily and inherently limited since, by the nature of these transactions, the patron is reposing that information in the library or bookstore and assumes the risk that the entity may disclose it to another. Whatever privacy interests a patron may have are outweighed by the Government's interest in obtaining the information in cases where the FBI can show the patron's relevance to an authorized full investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

# **EXHIBIT K**

# A Review of the Federal Bureau of Investigation's Use of National Security Letters



Office of the Inspector General  
March 2007

---

**UNCLASSIFIED**

## TABLE OF CONTENTS

TABLE OF CONTENTS .....	i
INDEX OF CHARTS, DIAGRAMS, AND TABLES.....	vi
LIST OF ACRONYMS .....	vii
EXECUTIVE SUMMARY .....	viii
CHAPTER ONE: INTRODUCTION .....	1
I.    Provisions of the USA Patriot Act and Reauthorization Act .....	1
II.   Methodology of the OIG Review .....	3
III.  Organization of the Report .....	5
CHAPTER TWO: BACKGROUND.....	7
I.    Background on National Security Letters .....	7
A.    The Patriot Act .....	8
B.    Types of Information Obtained by National Security Letters.....	10
C.    The Patriot Reauthorization Act .....	10
II.   The Four National Security Letter Statutes .....	11
A.    The Right to Financial Privacy Act .....	11
B.    The Electronic Communications Privacy Act .....	12
C.    The Fair Credit Reporting Act .....	14
D.    The National Security Act .....	15
III.  The Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection.....	16
A.    Levels of Investigative Activity under the FCI Guidelines (January 1, 2003 – October 31, 2003).....	16
B.    Levels of Investigative Activity under the NSI Guidelines (October 31, 2003).....	17
IV.  The Role of FBI Headquarters and Field Offices in Issuing and Using National Security Letters.....	18
A.    FBI Headquarters .....	18

1.	Counterterrorism Division.....	19
2.	Counterintelligence Division.....	19
3.	Cyber Division .....	19
4.	Directorate of Intelligence.....	19
5.	Office of the General Counsel (FBI-OGC) .....	20
B.	FBI Field Divisions .....	20
1.	Chief Division Counsel.....	20
2.	Field Intelligence Groups.....	21
CHAPTER THREE: THE FBI'S COLLECTION AND RETENTION OF INFORMATION OBTAINED FROM NATIONAL SECURITY LETTERS .....		22
I.	The FBI's Process for Collecting Information Through National Security Letters .....	22
II.	The FBI's Retention of Information Obtained from National Security Letters .....	27
CHAPTER FOUR: NATIONAL SECURITY LETTER REQUESTS ISSUED BY THE FBI FROM 2003 THROUGH 2005 .....		31
I.	Inaccuracies in the FBI's National Security Letter Tracking Database .....	31
II.	National Security Letter Requests From 2003 Through 2005.....	36
CHAPTER FIVE: THE EFFECTIVENESS OF NATIONAL SECURITY LETTERS AS AN INVESTIGATIVE TOOL.....		42
I.	Introduction .....	42
II.	The Effectiveness of National Security Letters Prior to the Patriot Act.....	43
III.	The Effectiveness of National Security Letters as an Investigative Tool in 2003 through 2005 .....	45
A.	The Importance of the Information Acquired From National Security Letters to the Department's Intelligence Activities .....	45
1.	Principal Uses of National Security Letters .....	46
2.	The Value of Each Type of National Security Letter.....	48

- B. Analysis of Information Obtained From National Security Letters..... 52
  - 1. Types of Analysis ..... 52
  - 2. Formal Analytical Intelligence Products ..... 54
- C. The FBI’s Dissemination of Information Obtained From National Security Letters to Other Entities..... 56
- D. Information From National Security Letters Provided to Law Enforcement Authorities for Use in Criminal Proceedings ..... 60
  - 1. Routine Information Sharing With United States Attorneys’ Offices ..... 60
  - 2. Providing Information to Law Enforcement Authorities for Use in Criminal Proceedings ..... 62
- IV. Conclusion ..... 65
- CHAPTER SIX: IMPROPER OR ILLEGAL USE OF NATIONAL SECURITY LETTER AUTHORITIES..... 66
- I. Possible IOB Violations Arising from National Security Letters Identified by the FBI ..... 67
  - A. The IOB Process for Reporting Possible Violations of Intelligence Activities in the United States ..... 68
  - B. Field Division Reports to FBI-OGC of 26 Possible IOB Violations Involving the Use of National Security Letters ..... 69
    - 1. Possible IOB Violations Identified by the FBI ..... 69
    - 2. OIG Analysis Regarding Possible IOB Violations Identified by the FBI..... 77
- II. Additional Possible IOB Violations Identified by the OIG During Our Field Visits..... 78
  - A. Possible IOB Violations Identified by the OIG..... 78
  - B. National Security Letter Issued in a Charlotte, N.C. Terrorism Investigation..... 82
  - C. OIG Analysis Regarding Possible IOB Violations Identified or Reviewed by the OIG ..... 84
- III. Improper Use of National Security Letter Authorities by Units in FBI Headquarters’ Counterterrorism Division Identified by the OIG ..... 86



A.	Using “Exigent Letters” Rather Than ECPA National Security Letters .....	86
1.	FBI Contracts With Three Telephone Companies .....	87
2.	The Exigent Letters to Three Telephone Companies.....	89
3.	Absence of Investigative Authority for the Exigent Letters .....	92
4.	Efforts by the FBI’s National Security Law Branch to Conform CAU’s Practices to the Electronic Communications Privacy Act.....	93
5.	OIG Analysis of Exigent Letters .....	95
B.	National Security Letters Issued From Headquarters Control Files Rather Than From Investigative Files.....	98
1.	National Security Letters Issued From a Headquarters Special Project Control File .....	98
2.	National Security Letters Issued by the Electronic Surveillance Operations and Sharing Unit.....	100
3.	OIG Analysis.....	102
IV.	Failure to Adhere to FBI Internal Control Policies on the Use of National Security Letter Authorities .....	103
1.	Lapses in Internal Controls .....	104
2.	OIG Analysis of Failures to Adhere to FBI Internal Control Policies .....	106
 CHAPTER SEVEN: OTHER NOTEWORTHY FACTS AND CIRCUMSTANCES RELATED TO THE FBI’S USE OF NATIONAL SECURITY LETTERS.....		
I.	Using the “least intrusive collection techniques feasible” .....	108
II.	Telephone “toll billing records information” .....	111
III.	The Role of FBI Division Counsel in Reviewing National Security Letters .....	112
IV.	Issuing NSLs From “Control Files” Rather Than From “Investigative Files” .....	115
V.	Obtaining Records From Federal Reserve Banks in Response to “Certificate Letters” Rather Than by Issuing RFPAs .....	115

VI. The OGC Database Does Not Identify the Targets of National Security Letters When They are Different From the Subjects of the Underlying Investigations..... 118

CHAPTER EIGHT: CONCLUSIONS AND RECOMMENDATIONS ..... 120

**[ Pages xi – xxvii omitted ]**

---

electronic surveillance on the subjects, leading to multiple convictions for conspiracy and providing material support to terrorists.

We learned from the responses that about half of the FBI's field divisions referred one or more counterterrorism investigation targets to law enforcement authorities for possible prosecution from 2003 through 2005. Of the 46 Headquarters and field divisions that responded to our request for information about referral of national security investigation targets, 19 divisions told us that they made no such referrals. Of the remaining 27 divisions, 22 divisions provided details about the type of information they referred and the nature of charges brought against these investigative subjects. In most cases, multiple charges were brought against the subjects, with the most common charges involving fraud (19), immigration (17), and money laundering (17).

#### **IV. Improper or Illegal Use of National Security Letter Authorities**

In this section of the Executive Summary, as directed by the Patriot Reauthorization Act, we report our findings on instances of "improper or illegal use" of national security letter authorities, including instances identified by the FBI as well as other instances identified by the OIG.<sup>26</sup>

##### **A. Field Division Reports to FBI-OGC of 26 Possible IOB Violations Involving the Use of National Security Letters**

The President's Intelligence Oversight Board (IOB) is directed by Executive Order 12863 to inform the President of any intelligence activities that "may be unlawful or contrary to Executive order or Presidential Directive." This directive has been interpreted by the Department and the IOB during the period covered by our review to include reports of violations of Department investigative guidelines or investigative procedures.<sup>27</sup>

We describe two groups of possible IOB violations related to NSLs that occurred during our review period (2003 through 2005). The first group

---

<sup>26</sup> In this report, we use the terms "improper or illegal use," as contained in the Patriot Reauthorization Act. As noted below, the improper or illegal uses of the national security letter authorities we found in our review did not involve criminal misconduct. However, as also noted below, the improper or illegal uses we found included serious misuses of national security letter authority.

<sup>27</sup> The FBI has developed an internal process for the self-reporting of possible IOB violations to FBI-OGC. During the period covered by our review, FBI-OGC issued 2 guidance memoranda describing the process by which FBI personnel were required to report such violations to FBI-OGC within 14 days of discovery. The reports were to include a description of the status of the subjects of the investigative activity, the legal authority for the investigation, the potential violation, and the date of the incident. FBI-OGC then reviewed the report, prepared a written opinion as to whether the matter should be sent to the IOB, and prepared the written communication to the IOB for those matters it decided to report.

consists of 26 possible IOB violations that were reported by FBI employees to FBI-OGC. The second group of incidents consists of 22 possible IOB violations which were not reported to FBI-OGC or the IOB that the OIG identified during our review of a sample of 77 investigative files in the 4 field divisions we visited.

### **1. Possible IOB Violations Identified by the FBI**

We determined that from 2003 through 2005, FBI field divisions reported 26 possible IOB violations to FBI-OGC arising from the use of national security letter authorities. The 26 possible IOB violations included:

- Three matters in which the NSLs were signed by the appropriate officials but the underlying investigations were not approved or extended by the appropriate Headquarters or field supervisors.
- Four matters in which the NSLs did not satisfy the requirements of the pertinent NSL statute or the applicable Attorney General Guidelines. In three of these matters, the FBI obtained the information without issuing NSLs. One of these three matters involved acquisition of telephone toll billing records in the absence of investigative authority under the Attorney General's NSI Guidelines. In the fourth matter, the FBI sought and obtained consumer full credit reports in a counterintelligence investigation, which is not permitted by the Patriot Act amendment to the FCRA, 15 U.S.C. § 1681v.
- Nineteen matters in which the NSL recipient provided more information than was requested in the NSL or provided information on the wrong person, due either to FBI typographical errors or errors by recipients of the NSLs. Thirteen of these matters involved requests for telephone toll billing records, 4 involved requests for electronic communication transactional records, and 2 involved requests for telephone subscriber information.

In 15 of the 26 matters identified by the FBI as possible IOB violations, the subject was a "U.S. person," and in 8 of the matters the subject was a "non-U.S. person." In one of the matters, the subject was a presumed "non-U.S. person," in one there was no subject because there was no underlying investigation, and in another the status of the subject could not be determined.

In total, 22 of the 26 possible IOB violations were due to FBI errors, while 4 were due to third-party errors. The FBI errors included typographical errors on the telephone numbers or e-mail addresses listed in the NSLs; telephone numbers that did not belong to the targets of NSLs; receipt of responses to three telephone toll billing record requests when the investigative authority was not properly authorized or had lapsed; receipt of telephone toll billing records and subscriber information from a telephone

company employee on nine separate occasions without issuing ECPA national security letters; and a FCRA NSL request for a consumer full credit report in a counterintelligence case. The errors also included instances in which the FBI obtained information without issuing the required NSL, including receipt of telephone toll billing records in the absence of an open national security investigation through informal contact with FBI Headquarters Counterterrorism Division's Communications Analysis Unit without issuing an ECPA NSL and accessing financial records through the use of FISA authorities rather than by issuing an RFPA NSL.

The four third-party errors included the NSL recipient providing prohibited content information (including voice messages) in response to an ECPA NSL for telephone toll billing records; and a third party providing prohibited content information (including e-mail content and images) in response to three ECPA NSLs requesting electronic communication transactional records.

Twenty of the 26 possible IOB violations were timely reported within 14 days of discovery to FBI-OGC in accordance with FBI policy. However, 6 were not reported in a timely fashion, taking between 15 days and 7 months to report. FBI records show that FBI-OGC reported 19 of the 26 possible violations to the IOB and decided not to report the 7 remaining matters.

## **2. OIG Analysis Regarding Possible IOB Violations Identified by the FBI**

Our examination of the 26 possible IOB violations reported to FBI-OGC did not reveal deliberate or intentional violations of NSL statutes, the Attorney General Guidelines, or internal FBI policy. Although the majority of the possible violations – 22 of 26 – arose from FBI errors, most of them occurred because of typographical errors or the case agent's good faith but erroneous belief that the information requested related to an investigative subject.

However, three of the possible IOB violations arising from FBI errors demonstrated FBI agents' unfamiliarity with the constraints on NSL authorities. In one instance, an FBI analyst was unaware of the statutory, Attorney General Guidelines, and internal FBI policy requirements that NSLs can only be issued during a national security investigation and must be signed by the Special Agent in Charge of the field division. In the two other matters, probationary agents erroneously believed that they were authorized to obtain records about investigative subjects – without issuing NSLs – from information derived from FISA electronic surveillance orders. In these instances, it is clear that the agents, and in one instance the squad supervisor, did not understand the interrelationship between FISA authorities and national security letter authorities.

With regard to the FBI's decisions whether to report the possible violations to the IOB, we concurred in FBI-OGC's analysis with one

exception. We disagreed with the FBI-OGC decision not to report the possible violation to the IOB related to the FBI's acquisition of telephone toll billing records and subscriber information relating to a "non-U.S. person" from a telephone company employee on nine occasions without issuing an NSL. FBI-OGC reasoned that because the investigative subject was a "non-U.S. person" agent of a foreign power, the only determination it had to reach was whether the FBI's failure to conform to its internal administrative requirements was reportable "as a matter of policy" to the IOB. In light of FBI-OGC's decisions to report at least four other IOB violations that were triggered by NSLs in which the investigative subject or the target of the NSL was a "non-U.S. person," we disagreed with FBI-OGC's determination that this matter should not be reported to the IOB.

**B. Additional Possible IOB Violations Arising From National Security Letters Identified by the OIG During Our Field Visits**

**1. Possible IOB Violations Identified by the OIG**

In addition to the 26 possible IOB violations identified by the FBI in this 3-year review period, we found 22 additional possible IOB violations during our review of 77 investigative files in the 4 field offices we visited.

In those 77 files, we reviewed 293 NSLs. We identified 22 NSL-related possible IOB violations that arose in the course of 17 separate investigations. None of these possible violations was reported to FBI-OGC or the IOB. Thus, we found that 22 percent of the investigative files we reviewed (17 of 77) contained one or more possible IOB violations that were not reported to FBI-OGC or the IOB.

The possible IOB violations we identified fell into three categories: improper authorization for the NSL (1), improper requests under the pertinent national security letter statutes (11), and unauthorized collections (10). The possible violations included:

- One NSL for telephone toll billing records was issued 22 days after the authorized period for the investigation had lapsed.
- Nine NSLs involved improper requests under the FCRA. Two of the 9 NSLs issued during one investigation requested consumer full credit reports during a counterintelligence investigation, while the statute authorizes this type of NSL only in international terrorism investigations. The approval ECs for 3 of these 9 NSLs listed FCRAv as the authority for the request but the NSLs included the certification of relevance language either for the RFPA or FCRAu NSL authorities. In addition, 4 of these 9 NSLs were FCRAv requests where the types of records approved by field supervisors differed from the records requested in the NSL.

- Two NSLs referenced the ECPA as authority for the request but sought content information not permitted by the statute. In one instance, the NSL requested information that arguably was content information and associated subscriber information.<sup>28</sup> The second NSL requested financial records associated with two e-mail addresses but requested the information under the ECPA rather than the RFPA, which only authorizes access to financial records.
- Ten NSLs involved the FBI's receipt of unauthorized information. In 4 instances, the FBI received telephone toll billing records or subscriber information for telephone numbers that were not listed in the national security letters. In these instances the provider either erroneously furnished additional records for another telephone number associated with the requested number or made transcription errors when querying its systems for the records. In 4 instances, the FBI received telephone toll billing records information and electronic communication transactional records for longer periods than that specified in the NSL – periods ranging from 30 days to 81 days. One NSL sought subscriber records pursuant to the ECPA, but the recipient provided the FBI with toll billing records. One NSL sought financial institution and consumer identifying information about an individual pursuant to FCRAu. However, the recipient erroneously gave the FBI the individual's consumer full credit report, which is available pursuant to another statute, FCRAv.

Twelve of the 22 possible IOB violations identified by the OIG were due to FBI errors, and 10 were due to errors on the part of third party recipients of the NSLs.<sup>29</sup>

---

<sup>28</sup> When we examined the records provided to the FBI in response to this NSL, however, we determined that the requested information was not furnished to the FBI.

<sup>29</sup> Our report also discusses another noteworthy possible IOB violation involving the issuance of an NSL seeking educational records from a North Carolina university. In that matter, which we learned of through press accounts, the FBI's Charlotte Division was in the process of seeking a grand jury subpoena for educational records about an investigative subject to determine whether the subject was involved in the July 2005 London subway and bus bombings. The NSL sought several categories of records, including applications for admission, housing information, emergency contacts, and campus health records. According to press accounts, university officials said that the FBI had tried to use an NSL to demand more information than the law permitted and declined to honor the national security letter. A grand jury subpoena was thereafter served on the university, and the university produced the records. In this instance, the FBI sought records it was not authorized to obtain pursuant to an ECPA national security letter.



## **2. OIG Analysis Regarding Possible IOB Violations Identified by the OIG**

In the limited file review we conducted of 77 investigative files in 4 FBI field offices, we identified nearly as many NSL-related possible IOB violations (22) as the number of NSL-related possible violations that the FBI identified (26) in reports from all FBI Headquarters and field divisions for the same 3-year period. We found that 22 percent of the investigative files that we reviewed contained at least one possible IOB violation that was not reported to FBI-OGC or the IOB. Because we have no reason to believe that the number of NSL-related possible IOB violations we identified in the four field offices was skewed or disproportionate to the number of possible IOB violations that exist in other offices, our findings suggest that a significant number of NSL-related possible IOB violations throughout the FBI have not been identified or reported by FBI personnel.

Our review did not reveal intentional violations of national security letter authorities, the Attorney General Guidelines, or internal FBI policy. Rather, we found confusion about the authorities available under the various NSL statutes. Our interviews of FBI field personnel and review of e-mail exchanges between NSLB attorneys and Division Counsel indicated that field personnel sometimes confused the two different authorities under the FCRA: the original FCRA provision that authorized access to financial institution and consumer identifying information in both counterterrorism and counterintelligence cases (15 U.S.C. §§ 1681u(a) and (b)), and the Patriot Act provision that amended the FCRA to authorize access to consumer full credit reports in international terrorism investigations where “such information is necessary for the agency’s conduct of such investigation, activity or analysis” (15 U.S.C. § 1681v). Although NSLB sent periodic guidance and “all CDC” e-mails to clarify the distinctions between the two NSLs, we found that the problems and confusion persisted.

In addition, we believe that many of the violations occurred because case agents and analysts do not consistently cross check the approval ECs with the text of proposed NSLs or verify upon receipt that the information supplied by the NSLs recipient matches the requests. We also question whether case agents or analysts reviewed the records provided by the NSL recipients to determine if records were received beyond the time period requested or, if they did so, determined that the amount of excess information received was negligible and did not need to be reported.

Our review also found that the FBI did not issue comprehensive guidance describing the types of NSL-related infractions that needed to be reported to FBI-OGC as possible IOB violations. We noted frequent exchanges between Division Counsel and NSLB attorneys about what should and should not be reported as possible IOB violations which we believe showed significant confusion about the reporting requirements. However, the FBI did not issue comprehensive guidance about NSL-related

infractions until November 2006, more than 5 years after the Patriot Act was enacted. We believe the lack of guidance contributed to the high rate of unreported possible IOB violations involving national security letters that we found.

As was the case with the NSL-related possible IOBs identified by the FBI, the possible violations identified or reviewed by the OIG varied in seriousness. Among the most serious matters resulting from FBI errors were the two NSLs requesting consumer full credit reports in a counterintelligence case and the NSL requesting educational records from a university, ostensibly pursuant to the ECPA. In these three instances, the FBI misused NSL authorities. Less serious infractions resulting from FBI errors were the seven matters in which three levels of supervisory review failed to detect and correct NSLs that contained incorrect certifications or sought records not referenced in the approval ECs. While the FBI was entitled to obtain the records sought or obtained in these seven NSLs, the lapses in oversight indicate that the FBI should reinforce the need for careful preparation and review of all documentation supporting the use of NSL authorities.

**C. Improper Use of National Security Letter Authorities by FBI Headquarters Counterterrorism Division Units Identified by the OIG**

We identified two ways in which FBI Headquarters Counterterrorism Division units circumvented the requirements of national security letter authorities or issued NSLs contrary to the Attorney General's NSI Guidelines and internal FBI policy. First, we learned 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. The letters stated the records were requested due to "exigent circumstances" and that subpoenas requesting the information had been submitted to the U.S. Attorney's Office for processing and service "as expeditiously as possible." However, in most instances there was no documentation associating the requests with pending national security investigations. In addition, while some witnesses told us that many of the exigent letters were issued in connection with fast-paced investigations, many were not issued in exigent circumstances, and the FBI was unable to determine which letters were sent in emergency circumstances due to inadequate recordkeeping. Further, in many instances after obtaining such records from the telephone companies, the FBI issued NSLs after the fact to "cover" the information obtained, but these after-the-fact NSLs sometimes were issued many months later.

Second, we determined that FBI Headquarters personnel regularly issued national security letters seeking electronic communication transactional records exclusively from “control files” rather than from “investigative files,” a practice not permitted under FBI policy. If NSLs are issued exclusively from control files, the NSL approval documentation does not indicate whether the NSLs are issued in the course of authorized investigations or whether the information sought in the NSLs is relevant to those investigations. Documentation of this information is necessary to establish compliance with NSL statutes, the Attorney General’s NSI Guidelines, and internal FBI policy.

We describe below these practices, how they were discovered, and what actions the FBI took to address the issues.

**1. Using “Exigent Letters” Rather Than ECPA National Security Letters**

The FBI entered into contracts with three telephone companies between May 2003 and March 2004 to obtain telephone toll billing records or subscriber information more quickly than by issuing ECPA NSLs. The requests for approval to obligate funds for each of these contracts referred to the Counterterrorism Division’s need to obtain telephone toll billing data from telephone companies as quickly as possible. The three memoranda stated that:

Previous methods of issuing subpoenas or National Security Letters (NSL) and having to wait weeks for their service, often via hard copy reports that had to be retyped into FBI databases, is insufficient to meet the FBI’s terrorism prevention mission.

The three memoranda also stated that the telephone companies would provide “near real-time servicing” of legal process, and that once legal process was served telephone records would be provided.

The Communications Analysis Unit (CAU) in the Counterterrorism Division’s Communications Exploitation Section (CXS) worked directly with telephone company representatives in connection with these contracts. CAU personnel told FBI employees that it expected to receive national security letters or other legal process before it obtained records from the telephone companies.

Using as its model a letter used by the FBI’s New York Division to request telephone records in connection with the FBI’s criminal investigations of the hijackers involved in the September 11 attacks, CAU issued over 700 exigent letters to the three telephone companies between

March 2003 and December 2005 that requested telephone toll billing records or subscriber information.<sup>30</sup> The letters stated:

Due to exigent circumstances, it is requested that records for the attached list of telephone numbers be provided. Subpoenas requesting this information have been submitted to the U.S. Attorney's Office who will process and serve them formally to [information redacted] as expeditiously as possible.

We determined that, contrary to the provisions of the contracts and the assertions in CAU's briefings that the FBI would obtain telephone records only after it served NSLs or grand jury subpoenas, the FBI obtained telephone toll billing records and subscriber information in response to the exigent letters prior to serving NSLs or grand jury subpoenas. Moreover, CAU officials told us that contrary to the assertion in the exigent letters, subpoenas requesting the information had not been provided to the U.S. Attorney's Office before the letters were sent to the telephone companies.

In total, between March 2003 and December 2005 the FBI issued at least 739 exigent letters to the three telephone companies requesting information on approximately 3,000 different telephone numbers. The exigent letters were signed by CXS Section Chiefs, CAU Unit Chiefs, and subordinate CAU personnel – including intelligence analysts – none of whom was delegated authority to sign NSLs.

CAU personnel told us that many of the exigent letters were generated in connection with significant Headquarters-based counterterrorism investigations as well as investigations in which the FBI provided assistance to foreign counterparts, such as investigations of the July 2005 London bombings, and that some CAU personnel believed some requests were urgent. However, when CAU personnel gave the exigent letters to the three telephone companies, they did not provide to their supervisors any documentation demonstrating that the requests related to pending FBI investigations. This documentation is necessary to establish compliance with the ECPA NSL statute, the NSI Guidelines, and internal FBI policy.

Moreover, when CAU requested telephone records from the three telephone companies pursuant to exigent letters, there sometimes were no open investigations tied to the request. In the absence of pending investigations, CAU sent leads either to the Headquarters Counterterrorism Division or to field offices that were geographically associated with the

---

<sup>30</sup> Following the September 11 attacks, the FBI's New York Division established a relationship with one of the major telephone companies to obtain quick responses to requests for telephone toll billing records or subscriber information in connection with its criminal investigations of the 19 hijackers. Although the New York Division generally obtained grand jury subpoenas to obtain this information, it frequently provided a "placeholder letter," sometimes referred to as an "exigent letter," to the telephone company if the grand jury subpoena was not yet available.

requests asking them to initiate new investigations from which the after-the-fact NSLs could be issued. However, Counterterrorism Division units and field personnel often resisted generating the documentation for these new investigations or declined to act on the leads, primarily for three reasons. First, CAU often did not provide the operating units with sufficient information to justify the initiation of an investigation. Second, on some occasions the documentation CAU supplied to the field divisions did not disclose that the FBI had already obtained the information from the telephone companies.<sup>31</sup> When the field offices learned that the records had already been received, they complained to attorneys in FBI-OGC's National Security Law Branch (NSLB) that this did not seem appropriate. Third, since Headquarters and field divisions were unfamiliar with the reasons underlying the requests, they believed that the CAU leads should receive lower priority than their ongoing investigations.

NSLB attorneys responsible for providing guidance on the FBI's use of national security letter authorities told us that they were not aware of CAU's practice of using exigent letters until late 2004. When an NSLB Assistant General Counsel learned of the practice at that time, she believed that the practice did not comply with the ECPA NSL statute. For nearly 2 years after learning of the practice, beginning in late 2004, NSLB attorneys counseled CAU officials to take a variety of actions, including: to discontinue use of exigent letters except in true emergencies; obtain more details to be able to justify associating the information with an existing national security investigation or to request the initiation of a new investigation; issue duly authorized NSLs promptly after the records were provided in response to the exigent letters; modify the letters to reference national security letters rather than grand jury subpoenas; and consider opening "umbrella" investigations out of which NSLs could be issued in the absence of another pending investigation. In addition, NSLB offered to dedicate personnel to expedite issuance of CAU NSL requests (as it had done for other high priority matters requiring expedited NSLs). However, CAU never pursued this latter option.

In addition, we found that the FBI did not maintain a log to track whether it issued NSLs or grand jury subpoenas after the fact to cover the records provided in response to the exigent letters, relying instead upon the three telephone companies to track whether NSLs or grand jury subpoenas were later issued. As a result, when we asked the FBI to match NSLs and grand jury subpoenas issued to the three telephone companies with a random sample of the exigent letters, the FBI was unable to provide reliable

---

<sup>31</sup> Similarly, when CAU on occasion asked the NSLB Deputy General Counsel to issue national security letters to cover information already obtained from the telephone companies in response to the exigent letters, CAU sometimes did not disclose in the approval documentation that the records already had been provided in response to the exigent letters. An NSLB Assistant General Counsel complained to CAU personnel about these omissions in December 2004.

evidence to substantiate that NSLs or other legal process was issued to cover the FBI's receipt of records requested in the sample exigent letters.

We also were troubled that the FBI issued exigent letters that contained factual misstatements indicating that “[s]ubpoenas requesting this information have been submitted to the U.S. Attorney’s Office who will process and serve them formally . . . as expeditiously as possible.”<sup>32</sup> In fact, in examining the documents CAU provided in support of the first 25 of the 88 randomly selected exigent letters, we could not confirm one instance in which a subpoena had been submitted to any United States Attorney’s Office before the exigent letter was sent to the telephone companies.

We concluded that, as a consequence of the CAU’s use of the exigent letters to acquire telephone toll billing records and subscriber information from three telephone companies without first issuing NSLs or grand jury subpoenas, the FBI circumvented the requirements of the ECPA NSL statute and violated the NSI Guidelines and internal FBI policies. These actions were compounded by the fact that CAU used exigent letters in non-emergency circumstances, failed to ensure that there were duly authorized investigations to which the requests could be tied, and failed to ensure that NSLs were issued promptly after the fact pursuant to existing or new counterterrorism investigations.

In evaluating these matters, it is also important to recognize the significant challenges the FBI was facing during the period covered by our review. After the September 11 terrorist attacks, the FBI implemented major organizational changes to seek to prevent additional terrorist attacks in the United States, such as overhauling its counterterrorism operations, expanding its intelligence capabilities, beginning to upgrade its information technology systems, and seeking to improve coordination with state and local law enforcement agencies. These changes occurred while the FBI and its Counterterrorism Division has had to respond to continuing terrorist threats and conduct many counterterrorism investigations, both internationally and domestically. In addition, the FBI developed specialized operational support units that were under significant pressure to respond quickly to potential terrorist threats. It was in this context that the FBI used exigent letters to acquire telephone toll billing records and subscriber information on approximately 3,000 different telephone numbers without first issuing ECPA national security letters. We also recognize that the FBI’s use of so-called “exigent letters” to obtain the records without first issuing NSLs was undertaken without the benefit of advance legal consultation with FBI-OGC.

---

<sup>32</sup> The FBI’s reference to grand jury subpoenas in the exigent letters rather than to national security letters appears to be the result of CAU’s use of the New York Division’s model letter for exigent letters sent to a telephone company in connection with the New York Division’s criminal investigations of the September 11 hijackers.

However, we believe none of these circumstances excuses the FBI's circumvention of the requirements of the ECPA NSL statute and its violations of the Attorney General's NSI Guidelines and internal FBI policy governing the use of national security letters.

## **2. National Security Letters Issued From Headquarters Control Files Rather Than From Investigative Files**

The national security letter statutes and the Attorney General's NSI Guidelines authorize the issuance of national security letters only if the information sought is relevant to an "authorized investigation." Within the FBI, the only types of investigations in which NSLs may be used are national security investigations.

For purposes of conducting its investigations and compiling information obtained from the use of various investigative authorities, agents may seek supervisory approval to establish an "investigative file." The FBI also provides for the establishment of non-investigative files, referred to as "control files" or "repository files," which are used to store information (such as the results of indices searches of the names of individuals who are relevant to FBI investigations) that may never rise to the level of predication necessary to initiate a national security investigation. The FBI's National Foreign Intelligence Program (NFIP) Manual states that control files are not investigative files and are not considered preliminary investigations or full investigations.

Unless national security letters are issued from investigative files, case agents and their supervisors – and internal and external reviewers – cannot determine whether the requests are tied to substantive investigations that have established the required evidentiary predicate for issuing NSLs. As the FBI General Counsel told us, the only way to determine if the information requested in a national security letter is relevant to an authorized investigation is to have an investigative file to which the NSL request can be tied or to have the connection described in the NSL approval EC.

Notwithstanding these policies, we found that in two circumstances the FBI relied exclusively on "control files" rather than "investigative files" to initiate approval for the issuance of many national security letters, in violation of FBI policy. In the first circumstance, from 2003 through 2005, CAU initiated NSL approval memoranda for approximately 300 national security letters in connection with a classified special project from a Headquarters control file. All of the resulting NSLs sought telephone toll billing records, subscriber information, or electronic communication transactional records pursuant to the ECPA NSL statute, but none of the approval ECs referred to the case number of any specific pending FBI investigation.

Since CAU officials are not authorized to sign NSLs, CAU sent leads to field offices to initiate the process to issue NSLs, but CAU met resistance from some field personnel who questioned the adequacy of predication to initiate a national security investigation.<sup>33</sup> To address the problem, the Counterterrorism Division opened a special project control file from which the CAU sought approval from NSLB to issue NSLs for subscriber information.

In December 2006, after considering a number of options that would comply with the ECPA NSL statute, the Attorney General's NSI Guidelines, and internal FBI policy, the FBI initiated an "umbrella" investigative file from which national security letters related to this classified project could be issued.

In the second circumstance, the FBI issued at least six national security letters from 2003 through 2005 solely on the authority of a control files established by the Counterterrorism Division's Electronic Surveillance Operations and Sharing Unit (EOPS) in the Communications Exploitation Section and another control file.<sup>34</sup> The six NSLs sought information from Internet service providers. None of the approval ECs accompanying the requests for these NSLs referred to the case number of any specific pending FBI investigation. Following questions raised by the OIG in this review, the NSLB Deputy General Counsel told us that she has advised the EOPS Unit Chief to discontinue requesting approval of national security letters issued exclusively out of control files.

#### **D. Failure to Adhere to FBI Internal Control Policies on the Use of National Security Letter Authorities**

During our field visits, we also examined FBI investigative files to determine whether the field office's use of national security letters violated FBI internal control policies. In our review of the 77 investigative files and 293 national security letters in 4 FBI field offices, we identified repeated failures to adhere to FBI-OGC guidance regarding the documentation necessary for approval of national security letters. Forty-six of the 77 files we examined (60 percent) contained one or more of the following infractions: (1) NSL approval memoranda that were not reviewed and initialed by one or more of the required field supervisors or Division Counsel; (2) NSL approval memoranda that did not contain the required information; and (3) NSLs that did not contain the certifications or other information required by the authorizing statutes.

---

<sup>33</sup> The classified nature of the project was such that few FBI Headquarters officials or FBI-OGC attorneys were authorized to know the predication for the requests.

<sup>34</sup> Problems with the FBI's NSL database make it impossible to determine the precise number of national security letters the FBI issued in this second category.



Approximately 7 percent of the approval memoranda we examined (22 of 293) did not reflect review or approval by one or more of the field supervisors who are required to approve NSL requests. They included failures to document approval by the Special Agents in Charge (4); Assistant Special Agents in Charge (18); Supervisory Special Agents (8); or the Chief Division Counsel or Assistant Division Counsel (3).

Thirty-four percent of the approval memoranda we examined (99 of 293) did not contain one or more of the four elements required by FBI internal policy. Approval memoranda failed to reference the statute authorizing the FBI to obtain the information or cited the wrong statute (16); failed to reference the “U.S. person” or “non-U.S. person” status of the investigative subject (66); failed to specify the type and number of records requested (34); and failed to recite the required predication for the request (7).

Approximately 2 percent of the national security letters we examined (5 of 293) did not include at least one of the required elements, including failures to reference an NSL statute or referencing the wrong statute. In addition, we were unable to comprehensively audit the field divisions’ compliance with the requirement that Special Agents in Charge sign national security letters because three of the four divisions we visited did not maintain signed copies of their national security letters. The Special Agent in Charge of the fourth division maintained a control file with copies of all NSLs he signs, but this practice was instituted only during the last year of our review period.

## **V. Other Noteworthy Fact and Circumstances Related to the FBI’s Use of National Security Letters**

As directed by the Patriot Reauthorization Act, our report includes “other noteworthy facts and circumstances” related to the FBI’s use of national security letters that we found during our review.

### **A. Using the “Least Intrusive Collection Techniques Feasible”**

The NSI Guidelines that were in effect during most of the period covered by our review state:

Choice of Methods. The conduct of investigations and other activities authorized by these Guidelines may present choices between the use of information collection methods that are more or less intrusive, considering such factors as the effect on the privacy of individuals and potential damage to reputation. As Executive Order 12333 § 2.4 provides, “the least intrusive collection techniques feasible” are to be used in such situations. The FBI shall not hesitate to use any lawful techniques consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness

[ Pages xlii – xlix; 1 – 6 omitted ]

---

## **CHAPTER TWO BACKGROUND**

In this chapter we describe the five national security letter authorities and the Attorney General Guidelines that govern their use. We also describe the roles of FBI Headquarters divisions and field components in issuing and using these letters in national security investigations.

### **I. Background on National Security Letters**

Over the last 20 years, Congress has enacted a series of laws authorizing the FBI to obtain certain types of information from third parties in terrorism, espionage, and classified information leak investigations without obtaining warrants from the Foreign Intelligence Surveillance Court or approval from another court.<sup>7</sup> These include five statutory provisions that authorize the FBI to obtain customer and consumer transactional information from communications providers, financial institutions, and consumer credit agencies by issuing national security letters (NSLs).<sup>8</sup> All but one of these provisions – the statute allowing access to consumer full credit reports in international terrorism investigations – predated the October 2001 passage of the Patriot Act. The authorizing statutes in effect prior to the Patriot Act required certification by a senior FBI Headquarters official that the FBI had “specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign

---

<sup>7</sup> FBI investigations of terrorism and espionage are called “national security investigations,” which are conducted pursuant to the Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (Oct. 31, 2003)(NSI Guidelines). NSLs are not authorized in connection with FBI conduct of ordinary criminal investigations or domestic terrorism investigations.

<sup>8</sup> The five statutes are:

- 1) 18 U.S.C. § 2709 (covering subscriber information and telephone toll billing records information and electronic communication transactional records);
- 2) 12 U.S.C. § 3414 (covering financial records);
- 3) 15 U.S.C. § 1681u (covering the names and addresses of all financial institutions at which a consumer maintains or has maintained an account; and the consumer’s name, address, former addresses, places of employment or former places of employment);
- 4) 15 U.S.C. § 1681v (covering consumer reports and all other information in a consumer’s file in international terrorism investigations); and
- 5) 50 U.S.C. § 436 (covering financial records, other financial information, and consumer reports in law enforcement investigations, counterintelligence inquiries, or security determinations). See Appendix A of this report for the text of the five statutes prior to the effective date of the Patriot Reauthorization Act.

The phrase “national security letter” was not used in any of the authorizing statutes, but was commonly used to refer to these authorities. The term was first used in legislation in the Patriot Reauthorization Act.

power or agent of a foreign power” as defined in the Foreign Intelligence Surveillance Act of 1978.<sup>9</sup>

### **A. The Patriot Act**

The September 11 attacks prompted a reevaluation of the law enforcement and intelligence tools that were available to detect and prevent terrorist attacks. Among the topics Congress and the Department of Justice considered was the use of national security letters.<sup>10</sup> The Department reported in Congressional testimony that “in many cases, counterintelligence and counterterrorism investigations suffer substantial delays while waiting for NSLs to be prepared, returned from Headquarters, and served.”<sup>11</sup>

The Patriot Act significantly expanded the FBI’s preexisting authority to obtain information through national security letters. Section 505 of the Patriot Act broadened the FBI’s authority by:

- Eliminating the requirement that the information sought in an NSL must pertain to a foreign power or an agent of a foreign power and substituting the lower threshold that the information requested be relevant to or sought for an investigation to protect against international terrorism or espionage, provided that the investigation of a United States person is not conducted “solely on the basis of activities protected by the first amendment of the Constitution of the United States”;
- Permitting, as a consequence of this lower threshold, national security letters to request information from communication providers, financial institutions, and consumer credit agencies

---

<sup>9</sup> See, e.g., 18 U.S.C. § 2709 (2000) ; 50 U.S.C. §§ 1801-1811 (2000).

<sup>10</sup> S. 1448, The Intelligence to Prevent Terrorism Act of 2001 and Other Legislative Proposals in the Wake of the September 11, 2001 Attacks: Hearing Before the Senate Select Comm. On Intelligence, 107<sup>th</sup> Cong. (2002); Dismantling the Financial Infrastructure of Global Terrorism: Hearing Before the House Comm. on Fin. Servs., 107<sup>th</sup> Cong. (2002); The Role of Technology in Preventing the Entry of Terrorists into the United States: Hearing Before the Senate Subcomm. on Tech., Terrorism, Gov’t Info. of the Comm. on the Judiciary, 107<sup>th</sup> Cong. (2002).

<sup>11</sup> Hearing Before the House Comm. on the Judiciary, 107<sup>th</sup> Cong. 57-58 (2001) (Administration’s Draft Anti-Terrorism Act of 2001). This view also was reflected in post-Patriot Act testimony at hearings considering whether to reauthorize the NSL authorities in the Patriot Act. See Tools Against Terror: How the Administration is Implementing New Laws in the Fight to Protect Our Homeland: Hearing Before the Subcomm. on Technology, Terrorism, and Gov’t Info. of the Senate Comm. on the Judiciary, 107<sup>th</sup> Cong. 139 (2002) (statement of Dennis Lormel, Chief, Terrorist Financing Operations Section, Counterterrorism Division, FBI)(“Delays in obtaining NSLs has long been identified as a significant problem relative to the conduct of counterintelligence and counterterrorism investigations.”)

about persons other than the subjects of FBI national security investigations so long as the requested information is relevant to an authorized investigation; and

- Permitting Special Agents in Charge of the FBI's 56 field offices to sign national security letters, thus significantly expanding approval authority beyond senior FBI Headquarters officials.<sup>12</sup>

In addition to expanding preexisting NSL authorities, the Patriot Act added a new NSL authority permitting the FBI and certain other federal government agencies to use NSLs to obtain access to consumer full credit reports in international terrorism investigations pursuant to an amendment to the Fair Credit Reporting Act (FCRA).<sup>13</sup> Prior to this amendment, the FBI could use FCRA NSLs only to obtain basic financial institution and consumer-identifying information about the person's bank accounts, places of employment, and addresses.<sup>14</sup>

The Patriot Act did not alter existing provisions in the statutes barring recipients of national security letters from disclosing their receipt of the letters and from disclosing the records provided. These so-called "gag order" provisions prohibited NSL recipients from challenging NSLs in court. Similarly, NSL authorities prior to the Patriot Act did not provide an express mechanism by which the FBI could enforce an NSL in court if a recipient refused to comply. The Patriot Act also did not include any express enforcement mechanism.

The pre-Patriot Act statutes required the FBI to provide classified semiannual reports to Congress disclosing summary information about national security letter usage.<sup>15</sup> The Patriot Act continued to require classified reports to Congress on the FBI's use of its NSL authorities.

---

<sup>12</sup> Prior to the Patriot Act, approximately 10 FBI Headquarters officials were authorized to sign national security letters, including the Director, Deputy Director, and the Assistant Directors and Deputy Assistant Directors of the Counterterrorism and Counterintelligence Divisions. Under the Patriot Act, the heads of the FBI's 56 field offices (Assistant Directors in Charge or Special Agents in Charge) may also issue NSLs. Since enactment of the Patriot Act, approval to sign NSLs has also been delegated to the Deputy Director, Executive Assistant Director (EAD), and Assistant EAD for the National Security Branch; Assistant Directors and all Deputy Assistant Directors for the Counterterrorism, Counterintelligence, and Cyber Divisions; all Special Agents in Charge of the New York, Washington, D.C., and Los Angeles field offices, which are headed by Assistant Directors in Charge; the General Counsel; and the Deputy General Counsel for the National Security Law Branch in the Office of the General Counsel.

<sup>13</sup> 15 U.S.C. § 1681v (Supp. IV 2005).

<sup>14</sup> 15 U.S.C. § 1681u (2000).

<sup>15</sup> The national security letter authority in the National Security Act, which allows collection of financial records and information, consumer reports, and travel records, did not require reports to Congress. See 50 U.S.C. § 436 (2000).

## **B. Types of Information Obtained by National Security Letters**

The type of information the FBI can obtain through national security letters includes:

### Telephone and e-mail Information

- Historical information on telephone calls made and received from a specified number, including land lines, cellular phones, prepaid phone card calls, toll free calls, alternate billed number calls (calls billed to third parties), and local and long distance billing records associated with the phone numbers (known as toll records);
- Electronic communication transactional records (e-mails), including e-mail addresses associated with the account; screen names; and billing records and method of payment; and
- Subscriber information associated with particular telephone numbers or e-mail addresses, such as the name, address, length of service, and method of payment.

### Financial Information

- Financial information such as information concerning open and closed checking and savings accounts and safe deposit box records from banks, credit unions, thrift institutions, investment banks or investment companies, as well as transactions with issuers of travelers checks, operators of credit card systems, pawnbrokers, loan or finance companies, travel agencies, real estate companies, casinos, and other entities.

### Consumer Credit Information

- Names and addresses of all financial institutions at which a consumer maintains or has maintained an account;
- Identifying information respecting a consumer . . . limited to name, address, former addresses, places of employment, or former places of employment; and
- Consumer reports of a consumer and all other information in a consumer's file (full credit reports).

## **C. The Patriot Reauthorization Act**

The Patriot Reauthorization Act reauthorized all of the provisions that were subject to lapse or “sunset” in the original Patriot Act (with some modification), including the five NSL authorities.<sup>16</sup> One of the modifications

---

<sup>16</sup> Pub. L. No. 109-177, § 102(a) (2006). The Patriot Reauthorization Act modified the non-disclosure requirements regarding national security letters. An NSL recipient may now disclose the NSL in connection with seeking legal advice or complying with the NSL. In

required the Department to issue, in addition to its semiannual classified reports, annual public reports that disclose certain data on the FBI's national security letter requests. The public report must include the aggregate number of NSL requests issued pursuant to the five NSL statutes including, for the first time, data on the use of the full credit report authority established pursuant to the Fair Credit Reporting Act, the only new NSL authority enacted by the Patriot Act.

The Department's first public annual report pursuant to the Patriot Reauthorization Act on the use of NSL authorities was issued on April 28, 2006.<sup>17</sup> The report stated that during calendar year 2005, federal government agencies issued 9,254 "NSL requests" involving 3,501 different "United States persons."<sup>18</sup>

## **II. The Four National Security Letter Statutes**

The following is a brief overview of the four statutes authorizing the FBI to issue five types of national security letters.

### **A. The Right to Financial Privacy Act**

The Right to Financial Privacy Act (RFPA) was enacted in 1978 "to protect the customers of financial institutions from unwarranted intrusion into their records while at the same time permitting legitimate law enforcement activity."<sup>19</sup> The RFPA requires federal government agencies to provide individuals with advance notice of requested disclosures of personal financial information and gives individuals an opportunity to challenge the request before disclosure is made to law enforcement authorities.<sup>20</sup>

The first NSL statute was passed in 1986 as an amendment to the RFPA. It created an exception to the advance notice requirement by permitting the FBI to obtain financial institution records in foreign

---

(cont'd.)

addition, the Patriot Reauthorization Act permits the NSL recipient to challenge compliance with the NSL and the non-disclosure requirement in federal court. In addition, the government may seek judicial enforcement of NSLs in the event of non-compliance.

<sup>17</sup> See Letter from William E. Moschella, Assistant Attorney General, to L. Ralph Mecham, Director, Administrative Office of the United States Courts (April 28, 2006), at 3.

<sup>18</sup> *Id.* In Chapter Four we describe the categories of NSL requests that are included and excluded from the public report.

<sup>19</sup> H.R. Rep. No. 95-1383, at 33 (1978), reprinted in 1978 U.S.C.C.A.N. 9273, 9305. The RFPA was enacted in response to the Supreme Court's decision in *United States v. Miller*, 425 U.S. 435 (1976), which held that customers of banking services had no expectation of privacy under the Fourth Amendment and therefore could not contest government access to their records.

<sup>20</sup> 12 U.S.C. §§ 3401-3422 (2000).

**[ Pages 12 – 126 and Appendix omitted ]**

---



# **EXHIBIT L**

**SEARCHING AND  
SEIZING COMPUTERS  
AND OBTAINING  
ELECTRONIC EVIDENCE  
IN CRIMINAL  
INVESTIGATIONS**

**Computer Crime and  
Intellectual Property Section  
Criminal Division**



**Published by  
Office of Legal Education  
Executive Office for  
United States Attorneys**

**H. Marshall Jarrett  
Director, EOUSA**

**Michael W. Bailie  
Director, OLE**

**OLE  
Litigation  
Series**

**Ed Hagen  
Assistant Director,  
OLE**

**Nathan Judish  
Computer Crime  
and Intellectual  
Property Section**

The Office of Legal Education intends that this book be used by Federal prosecutors for training and law enforcement purposes.

The contents of this book provide internal suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. See *United States v. Caceres*, 440 U.S. 741 (1979).

# Table of Contents

Preface and Acknowledgements .....	vii
Introduction.....	ix
<b>Chapter 1. Searching and Seizing Computers</b>	
<b>Without a Warrant.....</b>	<b>1</b>
A. Introduction.....	1
B. The Fourth Amendment’s “Reasonable Expectation of Privacy” in Cases Involving Computers .....	2
1. General Principles .....	2
2. Reasonable Expectation of Privacy in Computers as Storage Devices .....	2
3. Reasonable Expectation of Privacy and Third-Party Possession.....	6
4. Private Searches.....	10
5. Use of Specialized Technology to Obtain Information .....	14
C. Exceptions to the Warrant Requirement in Cases Involving Computers.....	15
1. Consent.....	15
2. Exigent Circumstances.....	27
3. Search Incident to a Lawful Arrest.....	31
4. Plain View.....	34
5. Inventory Searches .....	37
6. Border Searches.....	38
7. Probation and Parole .....	40
D. Special Case: Workplace Searches.....	42
1. Private-Sector Workplace Searches.....	42
2. Public-Sector Workplace Searches.....	45
E. International Issues .....	56
<b>Chapter 2. Searching and Seizing Computers</b>	
<b>With a Warrant.....</b>	<b>61</b>
A. Introduction.....	61
B. Devising a Search Strategy .....	61
C. Drafting the Affidavit, Application, and Warrant .....	63
1. Include Facts Establishing Probable Cause .....	63
2. Describe With Particularity the Things to be Seized .....	69

3. Establishing the Necessity for Imaging and Off-Site Examination .....	76
4. Do Not Place Limitations on the Forensic Techniques That May Be Used To Search .....	79
5. Seeking Authorization for Delayed Notification Search Warrants ...	83
6. Multiple Warrants in Network Searches .....	84
D. Forensic Analysis.....	86
1. The Two-Stage Search.....	86
2. Searching Among Commingled Records .....	87
3. Analysis Using Forensic Software.....	89
4. Changes of Focus and the Need for New Warrants.....	90
5. Permissible Time Period for Examining Seized Media.....	91
6. Contents of Rule 41(f) Inventory Filed With the Court .....	95
E. Challenges to the Search Process .....	96
1. Challenges Based on “Flagrant Disregard” .....	96
2. Motions for Return of Property.....	98
F. Legal Limitations on the Use of Search Warrants to Search Computers .....	100
1. Journalists and Authors: the Privacy Protection Act.....	101
2. Privileged Documents .....	109
3. Other Disinterested Third Parties .....	111
4. Communications Service Providers: the SCA.....	112
<b>Chapter 3. The Stored Communications Act .....</b>	<b>115</b>
A. Introduction.....	115
B. Providers of Electronic Communication Service vs. Remote Computing Service.....	117
1. Electronic Communication Service .....	117
2. Remote Computing Service.....	119
C. Classifying Types of Information Held by Service Providers.....	120
1. Basic Subscriber and Session Information Listed in 18 U.S.C. § 2703(c)(2) .....	121
2. Records or Other Information Pertaining to a Customer or Subscriber .....	122
3. Contents and “Electronic Storage” .....	122
4. Illustration of the SCA’s Classifications in the Email Context.....	125
D. Compelled Disclosure Under the SCA .....	127
1. Subpoena.....	128

- 2. Subpoena with Prior Notice to the Subscriber or Customer .....129
- 3. Section 2703(d) Order.....130
- 4. 2703(d) Order with Prior Notice to the Subscriber or Customer...132
- 5. Search Warrant.....133
- E. Voluntary Disclosure .....135
- F. Quick Reference Guide.....138
- G. Working with Network Providers: Preservation of Evidence,  
Preventing Disclosure to Subjects, Cable Act Issues,  
and Reimbursement.....139
  - 1. Preservation of Evidence under 18 U.S.C. § 2703(f) .....139
  - 2. Orders Not to Disclose the Existence of a Warrant,  
Subpoena, or Court Order.....140
  - 3. The Cable Act, 47 U.S.C. § 551 .....141
  - 4. Reimbursement.....142
- H. Constitutional Considerations .....144
- I. Remedies.....147
  - 1. Suppression .....147
  - 2. Civil Actions and Disclosures.....148

## Chapter 4. Electronic Surveillance in Communications

- Networks ..... 151**
- A. Introduction.....151
- B. Content vs. Addressing Information .....151
- C. The Pen/Trap Statute, 18 U.S.C. §§ 3121-3127.....153
  - 1. Definition of Pen Register and Trap and Trace Device .....153
  - 2. Pen/Trap Orders: Application, Issuance, Service, and Reporting...154
  - 3. Emergency Pen/Traps.....158
  - 4. The Pen/Trap Statute and Cell-Site Information.....159
- D. The Wiretap Statute (“Title III”), 18 U.S.C. §§ 2510-2522.....161
  - 1. Introduction: The General Prohibition.....161
  - 2. Key Phrases .....162
  - 3. Exceptions to Title III’s Prohibition .....167
- E. Remedies For Violations of Title III and the Pen/Trap Statute.....183
  - 1. Suppression Remedies .....183
  - 2. Defenses to Civil and Criminal Actions .....188

<b>Chapter 5. Evidence</b> .....	<b>191</b>
A. Introduction.....	191
B. Hearsay.....	191
1. Hearsay vs. Non-Hearsay Computer Records.....	192
2. Confrontation Clause.....	196
C. Authentication .....	197
1. Authentication of Computer-Stored Records .....	198
2. Authentication of Records Created by a Computer Process.....	200
3. Common Challenges to Authenticity .....	202
D. Other Issues .....	205
1. The Best Evidence Rule .....	205
2. Computer Printouts as “Summaries” .....	207
 <b>Appendices</b>	
A. Sample Network Banner Language.....	209
B. Sample 18 U.S.C. § 2703(d) Application and Order .....	213
C. Sample Language for Preservation Requests under 18 U.S.C. § 2703(f).....	225
D. Sample Pen Register/Trap and Trace Application and Order .....	227
E. Sample Subpoena Language.....	239
F. Sample Premises Computer Search Warrant Affidavit .....	241
G. Sample Letter for Provider Monitoring .....	251
H. Sample Authorization for Monitoring of Computer Trespasser Activity.....	253
I. Sample Email Account Search Warrant Affidavit .....	255
J. Sample Consent Form for Computer Search .....	263
 <b>Table of Cases</b> .....	<b>265</b>
 <b>Index</b> .....	<b>281</b>

**[ Pages v – 212 omitted ]**

# Appendix B

## Sample 18 U.S.C. § 2703(d) Application and Order

---

Note that this sample 2703(d) application and order are for the disclosure of both content and non-content information associated with an email account at an ISP.

When using a 2703(d) order to compel disclosure of content, the government is required either to give prior notice to the subscriber or customer or to comply with the procedures for delayed notice in 18 U.S.C. § 2705(a). This order authorizes the delay of notice to the account holder under 18 U.S.C. § 2705(a). A 2703(d) order can be used to compel disclosure of the content of communications not in “electronic storage” or the content of communications in “electronic storage” for more than 180 days. As discussed in Chapter 3.C.3, courts disagree on whether previously retrieved communications fall within the scope of communications in “electronic storage.”

When a 2703(d) order is used to compel disclosure only of non-content information, no notice to the customer or subscriber is required.

---

UNITED STATES DISTRICT COURT  
FOR THE [DISTRICT]

---

IN RE APPLICATION OF THE	)	
UNITED STATES OF AMERICA FOR	)	MISC. NO. _____
AN ORDER PURSUANT TO	)	
18 U.S.C. § 2703(d)	)	
	)	Filed Under Seal

---

APPLICATION OF THE UNITED STATES  
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, moving by and through its undersigned

---



counsel, respectfully submits under seal this ex parte application for an Order pursuant to 18 U.S.C. § 2703(d) to require ISPCoMpany, an Internet Service Provider located in City, State, which functions as an electronic communications service provider and/or a remote computing service, to provide records and other information and contents of wire or electronic communications pertaining to the following email account: sample@sample.com. The records and other information requested are set forth as an Attachment to the proposed Order. In support of this application, the United States asserts:

### LEGAL AND FACTUAL BACKGROUND

1. The United States government is investigating [crime summary]. The investigation concerns possible violations of, inter alia, [statutes].

2. Investigation to date of these incidents provides reasonable grounds to believe that ISPCoMpany has records and other information pertaining to certain of its subscribers that are relevant and material to an ongoing criminal investigation. Because ISPCoMpany functions as an electronic communications service provider (provides its subscribers access to electronic communication services, including email and the Internet) and/or a remote computing service (provides computer facilities for the storage and processing of electronic communications), 18 U.S.C. § 2703 sets out particular requirements that the government must meet in order to obtain access to the records and other information it is seeking.

3. Here, the government seeks to obtain the following categories of information: (1) records and other information (not including the contents of

communications) pertaining to certain subscribers of ISPCompany; and (2) the contents of electronic communications held by ISPCompany (but not in electronic storage for less than 181 days).

4. To obtain records and other information (not including the contents of communications) pertaining to subscribers of an electronic communications service provider or remote computing service, the government must comply with 18 U.S.C. § 2703(c)(1), which provides, in pertinent part:

A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

....

(B) obtains a court order for such disclosure under subsection (d) of this section.

5. Under 18 U.S.C. § 2703(a)(1) and 18 U.S.C. § 2703(b)(1), to obtain the contents of a wire or electronic communication in a remote computing service, or in electronic storage for more than one hundred and eighty days in an electronic communications system, the government must comply with 18 U.S.C. § 2703(b)(1), which provides, in pertinent part:

A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

....

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

....

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

6. Section 2703(b)(2) states that § 2703(b)(1) applies with respect to any wire or electronic communication that is held or maintained in a remote computing service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

7. Section 2703(d), in turn, provides in pertinent part:

A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction<sup>1</sup> and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. . . . A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually

---

<sup>1</sup> 18 U.S.C. § 2711(3) states that “the term ‘court of competent jurisdiction’ has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.” Section 3127 defines the term “court of competent jurisdiction” to include “any district court of the United States (including a magistrate judge of such a court).” 18 U.S.C. § 3127(2)(A).

voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

Accordingly, this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the materials sought are relevant and material to an ongoing criminal investigation.

#### THE RELEVANT FACTS

8. [Factual paragraph(s) here]

9. The conduct described above provides reasonable grounds to believe that the materials sought are relevant and material to an ongoing criminal investigation.

10. Records of customer and subscriber information relating to this investigation that are available from ISPCCompany, and the contents of electronic communications that may be found at ISPCCompany, will help government investigators to identify the individual(s) who are responsible for the events described above and to determine the nature and scope of their activities. Accordingly, the government requests that ISPCCompany be directed to produce all records described in Attachment A to the proposed Order. Part A of the Attachment requests the account name, address, telephone number, email address, billing information, and other identifying information for sample@sample.com.

11. Part B requests the production of records and other information relating to sample@sample.com through the date of this Court's Order. As described in more detail in that section, this information should include connection

information, telephone records, non-content information associated with any communication or file stored by or for the account(s), and correspondence and notes of records involving the account.

12. Part C requests the contents of electronic communications (not in electronic storage) in ISPCompany's computer systems in directories or files owned or controlled by the accounts identified in Part A. These stored files, covered by 18 U.S.C. § 2703(b)(2), will help ascertain the scope and nature of the activity conducted by sample@sample.com from ISPCompany's computers. Pursuant to 18 U.S.C. § 2703(a), Part C also requests the contents of electronic communications that have been in electronic storage in ISPCompany's computer systems for more than 180 days.

13. The information requested should be readily accessible to ISPCompany by computer search, and its production should not prove to be burdensome.

14. The United States requests that this application and Order be sealed by the Court until such time as the Court directs otherwise.

15. The United States requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), ISPCompany be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this Order for such period as the Court deems appropriate. The United States submits that such an order is justified because notification of the existence of this Order would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence,

change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.

16. The United States further requests, pursuant to the delayed notice provisions of 18 U.S.C. § 2705(a), an order delaying any notification to the subscriber or customer that may be required by § 2703(b) to obtain the contents of communications, for a period of ninety days. Providing prior notice to the subscriber or customer would seriously jeopardize the ongoing investigation, as such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.

WHEREFORE, it is respectfully requested that the Court grant the attached Order (1) directing ISPCCompany to provide the United States with the records and information described in Attachment A; (2) directing that the application and Order be sealed; (3) directing ISPCCompany not to disclose the existence or content of the Order or this investigation, except to the extent necessary to carry out the Order; and (4) directing that the notification by the government otherwise required under 18 U.S.C. § 2703(b) be delayed for ninety days; and (5) directing that three certified copies of this application and Order be provided by the Clerk of this Court to the United States Attorney's Office.

Executed on \_\_\_\_\_

\_\_\_\_\_  
Assistant United States Attorney

UNITED STATES DISTRICT COURT  
FOR THE \_\_\_\_\_

_____	)	
IN RE APPLICATION OF THE	)	
UNITED STATES OF AMERICA FOR	)	MISC. NO.
AN ORDER PURSUANT TO	)	
18 U.S.C. § 2703(d)	)	
_____	)	Filed Under Seal

**ORDER**

This matter having come before the Court pursuant to an application under Title 18, United States Code, Section 2703, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing ISPCo, an electronic communications service provider and/or a remote computing service, located in City, State, to disclose certain records and other information, as set forth in Attachment A to this Order, the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information and the contents of wire or electronic communications sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice to any person of this investigation or this application and Order entered in connection therewith would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that ISPCo will, within seven days of the date of this Order,

turn over to the United States the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three (3) certified copies of this application and Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that ISPCCompany shall not disclose the existence of the application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court.

IT IS FURTHER ORDERED that the notification by the government otherwise required under 18 U.S.C. § 2703(b)(1)(B) be delayed for a period of ninety days.

\_\_\_\_\_  
United States Magistrate Judge

\_\_\_\_\_  
Date



## ATTACHMENT A

You are to provide the following information, if available, as data files on CD-ROM or other electronic media or by facsimile:

- A. The following customer or subscriber account information for each account registered to or associated with sample@sample.com for the time period [date range]:
  1. subscriber names, user names, screen names, or other identities;
  2. mailing addresses, residential addresses, business addresses, email addresses, and other contact information;
  3. local and long distance telephone connection records, or records of session times and durations;
  4. length of service (including start date) and types of service utilized;
  5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
  6. means and source of payment for such service (including any credit card or bank account number) and billing records.
- B. All records and other information relating to the account(s) and time period in Part A, including:
  1. records of user activity for any connections made to or from the account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
  2. telephone records, including caller identification records, cellular site and sector information, GPS data, and cellular network identifying information (such as the IMSI, MSISDN, IMEI, MEID, or

- ESN);
3. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
  4. correspondence and notes of records related to the account(s).
- C. [Before seeking to compel disclosure of content, give prior notice to the customer or subscriber *or* comply with the delayed notice provisions of 18 U.S.C. § 2705(a).] The contents of electronic communications (not in electronic storage<sup>2</sup>) in ISPCompany’s systems in directories or files owned or controlled by the accounts identified in Part A at any time from [date range]; and the contents of electronic communications that have been in electronic storage in ISPCompany’s electronic communications system for more than 180 days [and within date range].

---

<sup>2</sup> “Electronic storage” is a term of art, specifically defined in 18 U.S.C. § 2510(17) as “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” The government does not seek access to any communications in “electronic storage” for less than 181 days. [The following sentence may not be included in the Ninth Circuit; see the discussion of “electronic storage” in Chapter 3.C.3.] Communications not in “electronic storage” include any email communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.

# **EXHIBIT M**

# The Washington Post

## The FBI's Secret Scrutiny

In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans

By Barton Gellman  
Washington Post Staff Writer  
Sunday, November 6, 2005

The FBI came calling in Windsor, Conn., this summer with a document marked for delivery by hand. On Matianuk Avenue, across from the tennis courts, two special agents found their man. They gave George Christian the letter, which warned him to tell no one, ever, what it said.

Under the shield and stars of the FBI crest, the letter directed Christian to surrender "all subscriber information, billing information and access logs of any person" who used a specific computer at a library branch some distance away. Christian, who manages digital records for three dozen Connecticut libraries, said in an affidavit that he configures his system for privacy. But the vendors of the software he operates said their databases can reveal the Web sites that visitors browse, the e-mail accounts they open and the books they borrow.

Christian refused to hand over those records, and his employer, Library Connection Inc., filed suit for the right to protest the FBI demand in public. The Washington Post established their identities -- still under seal in the U.S. Court of Appeals for the 2nd Circuit -- by comparing unsealed portions of the file with public records and information gleaned from people who had no knowledge of the FBI demand.

The Connecticut case affords a rare glimpse of an exponentially growing practice of domestic surveillance under the USA Patriot Act, which marked its fourth anniversary on Oct. 26. "National security letters," created in the 1970s for espionage and terrorism investigations, originated as narrow exceptions in consumer privacy law, enabling the FBI to review in secret the customer records of suspected foreign agents. 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.

The FBI now issues more than 30,000 national security letters a year, according to government sources, a hundredfold increase over historic norms. The letters -- one of which can be used to sweep up the records of many people -- are extending the bureau's reach as never before into the telephone calls, correspondence and financial lives of ordinary Americans.

Issued by FBI field supervisors, national security letters do not need the imprimatur of a prosecutor, grand jury or judge. They receive no review after the fact by the Justice Department or Congress. The executive branch maintains only statistics, which are incomplete and confined to classified reports. The Bush administration defeated legislation and a lawsuit to require a public accounting, and has offered no example in which the use of a national security letter helped disrupt a terrorist plot.

The burgeoning use of national security letters coincides with an unannounced decision to deposit all

the information they yield into government data banks -- and to share those private records widely, in the federal government and beyond. In late 2003, the Bush administration reversed a long-standing policy requiring agents to destroy their files on innocent American citizens, companies and residents when investigations closed. Late last month, President Bush signed Executive Order 13388, expanding access to those files for "state, local and tribal" governments and for "appropriate private sector entities," which are not defined.

National security letters offer a case study of the impact of the Patriot Act outside the spotlight of political debate. Drafted in haste after the Sept. 11, 2001, attacks, the law's 132 pages wrought scores of changes in the landscape of intelligence and law enforcement. Many received far more attention than the amendments to a seemingly pedestrian power to review "transactional records." But few if any other provisions touch as many ordinary Americans without their knowledge.

Senior FBI officials acknowledged in interviews that the proliferation of national security letters results primarily from the bureau's new authority to collect intimate facts about people who are not suspected of any wrongdoing. Criticized for failure to detect the Sept. 11 plot, the bureau now casts a much wider net, using national security letters to generate leads as well as to pursue them. Casual or unwitting contact with a suspect -- a single telephone call, for example -- may attract the attention of investigators and subject a person to scrutiny about which he never learns.

A national security letter cannot be used to authorize eavesdropping or to read the contents of e-mail. But it does permit investigators to trace revealing paths through the private affairs of a modern digital citizen. The records it yields describe where a person makes and spends money, with whom he lives and lived before, how much he gambles, what he buys online, what he pawns and borrows, where he travels, how he invests, what he searches for and reads on the Web, and who telephones or e-mails him at home and at work.

As it wrote the Patriot Act four years ago, Congress bought time and leverage for oversight by placing an expiration date on 16 provisions. The changes involving national security letters were not among them. In fact, as the Dec. 31 deadline approaches and Congress prepares to renew or make permanent the expiring provisions, House and Senate conferees are poised again to amplify the FBI's power to compel the secret surrender of private records.

The House and Senate have voted to make noncompliance with a national security letter a criminal offense. The House would also impose a prison term for breach of secrecy.

Like many Patriot Act provisions, the ones involving national security letters have been debated in largely abstract terms. The Justice Department has offered Congress no concrete information, even in classified form, save for a partial count of the number of letters delivered. The statistics do not cover all forms of national security letters or all U.S. agencies making use of them.

"The beef with the NSLs is that they don't have even a pretense of judicial or impartial scrutiny," said former representative Robert L. Barr Jr. (Ga.), who finds himself allied with the American Civil Liberties Union after a career as prosecutor, CIA analyst and conservative GOP stalwart. "There's no checks and balances whatever on them. It is simply some bureaucrat's decision that they want information, and they can basically just go and get it."

## 'A Routine Tool'

Career investigators and Bush administration officials emphasized, in congressional testimony and interviews for this story, that national security letters are for hunting terrorists, not fishing through the private lives of the innocent. The distinction is not as clear in practice.

Under the old legal test, the FBI had to have "specific and articulable" reasons to believe the records it gathered in secret belonged to a terrorist or a spy. Now the bureau needs only to certify that the records are "sought for" or "relevant to" an investigation "to protect against international terrorism or clandestine intelligence activities."

That standard enables investigators to look for conspirators by sifting the records of nearly anyone who crosses a suspect's path.

"If you have a list of, say, 20 telephone numbers that have come up . . . on a bad guy's telephone," said Valerie E. Caproni, the FBI's general counsel, "you want to find out who he's in contact with." Investigators will say, " 'Okay, phone company, give us subscriber information and toll records on these 20 telephone numbers,' and that can easily be 100."

Bush administration officials compare national security letters to grand jury subpoenas, which are also based on "relevance" to an inquiry. There are differences. Grand juries tend to have a narrower focus because they investigate past conduct, not the speculative threat of unknown future attacks. Recipients of grand jury subpoenas are generally free to discuss the subpoenas publicly. And there are strict limits on sharing grand jury information with government agencies.

Since the Patriot Act, the FBI has dispersed the authority to sign national security letters to more than five dozen supervisors -- the special agents in charge of field offices, the deputies in New York, Los Angeles and Washington, and a few senior headquarters officials. FBI rules established after the Patriot Act allow the letters to be issued long before a case is judged substantial enough for a "full field investigation." Agents commonly use the letters now in "preliminary investigations" and in the "threat assessments" that precede a decision whether to launch an investigation.

"Congress has given us this tool to obtain basic telephone data, basic banking data, basic credit reports," said Caproni, who is among the officials with signature authority. "The fact that a national security letter is a routine tool used, that doesn't bother me."

If agents had to wait for grounds to suspect a person of ill intent, said Joseph Billy Jr., the FBI's deputy assistant director for counterterrorism, they would already know what they want to find out with a national security letter. "It's all chicken and egg," he said. "We're trying to determine if someone warrants scrutiny or doesn't."

Billy said he understands that "merely being in a government or FBI database . . . gives everybody, you know, neck hair standing up." Innocent Americans, he said, "should take comfort at least knowing that it is done under a great deal of investigative care, oversight, within the parameters of the law."

He added: "That's not going to satisfy a majority of people, but . . . I've had people say, you know, 'Hey, I don't care, I've done nothing to be concerned about. You can have me in your files and that's

that.' Some people take that approach."

### **'Don't Go Overboard'**

In Room 7975 of the J. Edgar Hoover Building, around two corners from the director's suite, the chief of the FBI's national security law unit sat down at his keyboard about a month after the Patriot Act became law. Michael J. Woods had helped devise the FBI wish list for surveillance powers. Now he offered a caution.

"NSLs are powerful investigative tools, in that they can compel the production of substantial amounts of relevant information," he wrote in a Nov. 28, 2001, "electronic communication" to the FBI's 56 field offices. "However, they must be used judiciously." Standing guidelines, he wrote, "require that the FBI accomplish its investigations through the 'least intrusive' means. . . . The greater availability of NSLs does not mean that they should be used in every case."

Woods, who left government service in 2002, added a practical consideration. Legislators granted the new authority and could as easily take it back. When making that decision, he wrote, "Congress certainly will examine the manner in which the FBI exercised it."

Looking back last month, Woods was struck by how starkly he misjudged the climate. The FBI disregarded his warning, and no one noticed.

"This is not something that should be automatically done because it's easy," he said. "We need to be sure . . . we don't go overboard."

One thing Woods did not anticipate was then-Attorney General John D. Ashcroft's revision of Justice Department guidelines. On May 30, 2002, and Oct. 31, 2003, Ashcroft rewrote the playbooks for investigations of terrorist crimes and national security threats. He gave overriding priority to preventing attacks by any means available.

Ashcroft remained bound by Executive Order 12333, which requires the use of the "least intrusive means" in domestic intelligence investigations. But his new interpretation came close to upending the mandate. Three times in the new guidelines, Ashcroft wrote that the FBI "should consider . . . less intrusive means" but "should not hesitate to use any lawful techniques . . . even if intrusive" when investigators believe them to be more timely. "This point," he added, "is to be particularly observed in investigations relating to terrorist activities."

### **'Why Do You Want to Know?'**

As the Justice Department prepared congressional testimony this year, FBI headquarters searched for examples that would show how expanded surveillance powers made a difference. Michael Mason, who runs the Washington field office and has the rank of assistant FBI director, found no ready answer.

"I'd love to have a made-for-Hollywood story, but I don't have one," Mason said. "I am not even sure such an example exists."

What national security letters give his agents, Mason said, is speed.

"I have 675 terrorism cases," he said. "Every one of these is a potential threat. And anything I can do to get to the bottom of any one of them more quickly gets me closer to neutralizing a potential threat."

Because recipients are permanently barred from disclosing the letters, outsiders can make no assessment of their relevance to Mason's task.

Woods, the former FBI lawyer, said secrecy is essential when an investigation begins because "it would defeat the whole purpose" to tip off a suspected terrorist or spy, but national security seldom requires that the secret be kept forever. Even mobster "John Gotti finds out eventually that he was wiretapped" in a criminal probe, said Peter Swire, the federal government's chief privacy counselor until 2001. "Anyone caught up in an NSL investigation never gets notice."

To establish the "relevance" of the information they seek, agents face a test so basic it is hard to come up with a plausible way to fail. A model request for a supervisor's signature, according to internal FBI guidelines, offers this one-sentence suggestion: "This subscriber information is being requested to determine the individuals or entities that the subject has been in contact with during the past six months."

Edward L. Williams, the chief division counsel in Mason's office, said that supervisors, in practice, "aren't afraid to ask . . . 'Why do you want to know?' " He would not say how many requests, if any, are rejected.

### **'The Abuse Is in the Power Itself'**

Those who favor the new rules maintain -- as Sen. Pat Roberts (R-Kan.), chairman of the Senate Select Committee on Intelligence, put it in a prepared statement -- that "there has not been one substantiated allegation of abuse of these lawful intelligence tools."

What the Bush administration means by abuse is unauthorized use of surveillance data -- for example, to blackmail an enemy or track an estranged spouse. Critics are focused elsewhere. What troubles them is not unofficial abuse but the official and routine intrusion into private lives.

To Jeffrey Breinholt, deputy chief of the Justice Department's counterterrorism section, the civil liberties objections "are eccentric." Data collection on the innocent, he said, does no harm unless "someone [decides] to act on the information, put you on a no-fly list or something." Only a serious error, he said, could lead the government, based on nothing more than someone's bank or phone records, "to freeze your assets or go after you criminally and you suffer consequences that are irreparable." He added: "It's a pretty small chance."

"I don't necessarily want somebody knowing what videos I rent or the fact that I like cartoons," said Mason, the Washington field office chief. But if those records "are never used against a person, if they're never used to put him in jail, or deprive him of a vote, et cetera, then what is the argument?"

Barr, the former congressman, said that "the abuse is in the power itself."



"As a conservative," he said, "I really resent an administration that calls itself conservative taking the position that the burden is on the citizen to show the government has abused power, and otherwise shut up and comply."

At the ACLU, staff attorney Jameel Jaffer spoke of "the profound chilling effect" of this kind of surveillance: "If the government monitors the Web sites that people visit and the books that they read, people will stop visiting disfavored Web sites and stop reading disfavored books. The FBI should not have unchecked authority to keep track of who visits [al-Jazeera's Web site] or who visits the Web site of the Federalist Society."

### **Links in a Chain**

Ready access to national security letters allows investigators to employ them routinely for "contact chaining."

"Starting with your bad guy and his telephone number and looking at who he's calling, and [then] who they're calling," the number of people surveilled "goes up exponentially," acknowledged Caproni, the FBI's general counsel.

But Caproni said it would not be rational for the bureau to follow the chain too far. "Everybody's connected" if investigators keep tracing calls "far enough away from your targeted bad guy," she said. "What's the point of that?"

One point is to fill government data banks for another investigative technique. That one is called "link analysis," a practice Caproni would neither confirm nor deny.

Two years ago, Ashcroft rescinded a 1995 guideline directing that information obtained through a national security letter about a U.S. citizen or resident "shall be destroyed by the FBI and not further disseminated" if it proves "not relevant to the purposes for which it was collected." Ashcroft's new order was that "the FBI shall retain" all records it collects and "may disseminate" them freely among federal agencies.

The same order directed the FBI to develop "data mining" technology to probe for hidden links among the people in its growing cache of electronic files. According to an FBI status report, the bureau's office of intelligence began operating in January 2004 a new Investigative Data Warehouse, based on the same Oracle technology used by the CIA. The CIA is generally forbidden to keep such files on Americans.

Data mining intensifies the impact of national security letters, because anyone's personal files can be scrutinized again and again without a fresh need to establish relevance.

"The composite picture of a person which emerges from transactional information is more telling than the direct content of your speech," said Woods, the former FBI lawyer. "That's certainly not been lost on the intelligence community and the FBI."

Ashcroft's new guidelines allowed the FBI for the first time to add to government files consumer data from commercial providers such as LexisNexis and ChoicePoint Inc. Previous attorneys general had

decided that such a move would violate the Privacy Act. In many field offices, agents said, they now have access to ChoicePoint in their squad rooms.

What national security letters add to government data banks is information that no commercial service can lawfully possess. Strict privacy laws, for example, govern financial and communications records. National security letters -- along with the more powerful but much less frequently used secret subpoenas from the Foreign Intelligence Surveillance Court -- override them.

### **'What Happens in Vegas'**

The bureau displayed its ambition for data mining in an emergency operation at the end of 2003.

The Department of Homeland Security declared an orange alert on Dec. 21 of that year, in part because of intelligence that hinted at a New Year's Eve attack in Las Vegas. The identities of the plotters were unknown.

The FBI sent Gurvais Grigg, chief of the bureau's little-known Proactive Data Exploitation Unit, in an audacious effort to assemble a real-time census of every visitor in the nation's most-visited city. An average of about 300,000 tourists a day stayed an average of four days each, presenting Grigg's team with close to a million potential suspects in the ensuing two weeks.

A former stockbroker with a degree in biochemistry, Grigg declined to be interviewed. Government and private sector sources who followed the operation described epic efforts to vacuum up information.

An interagency task force began pulling together the records of every hotel guest, everyone who rented a car or truck, every lease on a storage space, and every airplane passenger who landed in the city. Grigg's unit filtered that population for leads. Any link to the known terrorist universe -- a shared address or utility account, a check deposited, a telephone call -- could give investigators a start.

"It was basically a manhunt, and in circumstances where there is a manhunt, the most effective way of doing that was to scoop up a lot of third party data and compare it to other data we were getting," Breinholt said.

Investigators began with emergency requests for help from the city's sprawling hospitality industry. "A lot of it was done voluntary at first," said Billy, the deputy assistant FBI director.

According to others directly involved, investigators turned to national security letters and grand jury subpoenas when friendly persuasion did not work.

Early in the operation, according to participants, the FBI gathered casino executives and asked for guest lists. The MGM Mirage company, followed by others, balked.

"Some casinos were saying no to consent [and said], 'You have to produce a piece of paper,' " said Jeff Jonas, chief scientist at IBM Entity Analytics, who previously built data management systems for casino surveillance. "They don't just market 'What happens in Vegas stays in Vegas.' They want it to be true."

The operation remained secret for about a week. Then casino sources told Rod Smith, gaming editor of the Las Vegas Review-Journal, that the FBI had served national security letters on them. In an interview for this article, one former casino executive confirmed the use of a national security letter. Details remain elusive. Some law enforcement officials, speaking on the condition of anonymity because they had not been authorized to divulge particulars, said they relied primarily on grand jury subpoenas. One said in an interview that national security letters may eventually have been withdrawn. Agents encouraged voluntary disclosures, he said, by raising the prospect that the FBI would use the letters to gather something more sensitive: the gambling profiles of casino guests. Caproni declined to confirm or deny that account.

What happened in Vegas stayed in federal data banks. Under Ashcroft's revised policy, none of the information has been purged. For every visitor, Breinholt said, "the record of the Las Vegas hotel room would still exist."

Grigg's operation found no suspect, and the orange alert ended on Jan. 10, 2004. "The whole thing washed out," one participant said.

### **'Of Interest to President Bush'**

At around the time the FBI found George Christian in Connecticut, agents from the bureau's Charlotte field office paid an urgent call on the chemical engineering department at North Carolina State University in Raleigh. They were looking for information about a former student named Magdy Nashar, then suspected in the July 7 London subway bombing but since cleared of suspicion.

University officials said in interviews late last month that the FBI tried to use a national security letter to demand much more information than the law allows.

David T. Drooz, the university's senior associate counsel, said special authority is required for the surrender of records protected by educational and medical privacy. The FBI's first request, a July 14 grand jury subpoena, did not appear to supply that authority, Drooz said, and the university did not honor it. Referring to notes he took that day, Drooz said Eric Davis, the FBI's top lawyer in Charlotte, "was focused very much on the urgency" and "he even indicated the case was of interest to President Bush."

The next day, July 15, FBI agents arrived with a national security letter. Drooz said it demanded all records of Nashar's admission, housing, emergency contacts, use of health services and extracurricular activities. University lawyers "looked up what law we could on the fly," he said. They discovered that the FBI was demanding files that national security letters have no power to obtain. The statute the FBI cited that day covers only telephone and Internet records.

"We're very eager to comply with the authorities in this regard, but we needed to have what we felt was a legally valid procedure," said Larry A. Neilsen, the university provost.

Soon afterward, the FBI returned with a new subpoena. It was the same as the first one, Drooz said, and the university still had doubts about its legal sufficiency. This time, however, it came from New York and summoned Drooz to appear personally. The tactic was "a bit heavy-handed," Drooz said, "the implication being you're subject to contempt of court." Drooz surrendered the records.

The FBI's Charlotte office referred questions to headquarters. A high-ranking FBI official, who spoke on the condition of anonymity, acknowledged that the field office erred in attempting to use a national security letter. Investigators, he said, "were in a big hurry for obvious reasons" and did not approach the university "in the exact right way."

### 'Unreasonable' or 'Oppressive'

The electronic docket in the Connecticut case, as the New York Times first reported, briefly titled the lawsuit *Library Connection Inc. v. Gonzales*. Because identifying details were not supposed to be left in the public file, the court soon replaced the plaintiff's name with "John Doe."

George Christian, Library Connection's executive director, is identified in his affidavit as "John Doe 2." In that sworn statement, he said people often come to libraries for information that is "highly sensitive, embarrassing or personal." He wanted to fight the FBI but feared calling a lawyer because the letter said he could not disclose its existence to "any person." He consulted Peter Chase, vice president of Library Connection and chairman of a state intellectual freedom committee. Chase -- "John Doe 1" in his affidavit -- advised Christian to call the ACLU. Reached by telephone at their homes, both men declined to be interviewed.

U.S. District Judge Janet C. Hall ruled in September that the FBI gag order violates Christian's, and Library Connection's, First Amendment rights. A three-judge panel heard oral argument on Wednesday in the government's appeal.

The central facts remain opaque, even to the judges, because the FBI is not obliged to describe what it is looking for, or why. During oral argument in open court on Aug. 31, Hall said one government explanation was so vague that "if I were to say it out loud, I would get quite a laugh here." After the government elaborated in a classified brief delivered for her eyes only, she wrote in her decision that it offered "nothing specific."

The Justice Department tried to conceal the existence of the first and only other known lawsuit against a national security letter, also brought by the ACLU's Jaffer and Ann Beeson. Government lawyers opposed its entry into the public docket of a New York federal judge. They have since tried to censor nearly all the contents of the exhibits and briefs. They asked the judge, for example, to black out every line of the affidavit that describes the delivery of the national security letter to a New York Internet company, including, "I am a Special Agent of the Federal Bureau of Investigation ('FBI')."

U.S. District Judge Victor Marrero, in a ruling that is under appeal, held that the law authorizing national security letters violates the First and Fourth Amendments.

Resistance to national security letters is rare. Most of them are served on large companies in highly regulated industries, with business interests that favor cooperation. The in-house lawyers who handle such cases, said Jim Dempsey, executive director of the Center for Democracy and Technology, "are often former prosecutors -- instinctively pro-government but also instinctively by-the-books." National security letters give them a shield against liability to their customers.

Kenneth M. Breen, a partner at the New York law firm Fulbright & Jaworski, held a seminar for corporate lawyers one recent evening to explain the "significant risks for the non-compliant" in

government counterterrorism investigations. A former federal prosecutor, Breen said failure to provide the required information could create "the perception that your company didn't live up to its duty to fight terrorism" and could invite class-action lawsuits from the families of terrorism victims. In extreme cases, he said, a business could face criminal prosecution, "a 'death sentence' for certain kinds of companies."

The volume of government information demands, even so, has provoked a backlash. Several major business groups, including the National Association of Manufacturers and the U.S. Chamber of Commerce, complained in an Oct. 4 letter to senators that customer records can "too easily be obtained and disseminated" around the government. National security letters, they wrote, have begun to impose an "expensive and time-consuming burden" on business.

The House and Senate bills renewing the Patriot Act do not tighten privacy protections, but they offer a concession to business interests. In both bills, a judge may modify a national security letter if it imposes an "unreasonable" or "oppressive" burden on the company that is asked for information.

### **'A Legitimate Question'**

As national security letters have grown in number and importance, oversight has not kept up. In each house of Congress, jurisdiction is divided between the judiciary and intelligence committees. None of the four Republican chairmen agreed to be interviewed.

Roberts, the Senate intelligence chairman, said in a statement issued through his staff that "the committee is well aware of the intelligence value of the information that is lawfully collected under these national security letter authorities," which he described as "non-intrusive" and "crucial to tracking terrorist networks and detecting clandestine intelligence activities." Senators receive "valuable reporting by the FBI," he said, in "semi-annual reports [that] provide the committee with the information necessary to conduct effective oversight."

Roberts was referring to the Justice Department's classified statistics, which in fact have been delivered three times in four years. They include the following information: how many times the FBI issued national security letters; whether the letters sought financial, credit or communications records; and how many of the targets were "U.S. persons." The statistics omit one whole category of FBI national security letters and also do not count letters issued by the Defense Department and other agencies.

Committee members have occasionally asked to see a sampling of national security letters, a description of their fruits or examples of their contribution to a particular case. The Justice Department has not obliged.

In 2004, the conference report attached to the intelligence authorization bill asked the attorney general to "include in his next semiannual report" a description of "the scope of such letters" and the "process and standards for approving" them. More than a year has passed without a Justice Department reply.

"The committee chairman has the power to issue subpoenas" for information from the executive branch, said Rep. Zoe Lofgren (D-Calif.), a House Judiciary Committee member. "The minority has no power to compel, and . . . Republicans are not going to push for oversight of the Republicans."

That's the story of this Congress."

In the executive branch, no FBI or Justice Department official audits the use of national security letters to assess whether they are appropriately targeted, lawfully applied or contribute important facts to an investigation.

Justice Department officials noted frequently this year that Inspector General Glenn A. Fine reports twice a year on abuses of the Patriot Act and has yet to substantiate any complaint. (One investigation is pending.) Fine advertises his role, but there is a puzzle built into the mandate. Under what scenario could a person protest a search of his personal records if he is never notified?

"We do rely upon complaints coming in," Fine said in House testimony in May. He added: "To the extent that people do not know of anything happening to them, there is an issue about whether they can complain. So, I think that's a legitimate question."

Asked more recently whether Fine's office has conducted an independent examination of national security letters, Deputy Inspector General Paul K. Martin said in an interview: "We have not initiated a broad-based review that examines the use of specific provisions of the Patriot Act."

At the FBI, senior officials said the most important check on their power is that Congress is watching.

"People have to depend on their elected representatives to do the job of oversight they were elected to do," Caproni said. "And we think they do a fine job of it."

*Researcher Julie Tate and research editor Lucy Shackelford contributed to this report.*

[View all comments](#) that have been posted about this article.

© 2005 The Washington Post Company

**EXHIBIT N**

**THE WALL STREET JOURNAL.**

WSJ.com

---

July 17, 2012, 10:41 PM ET

# What It's Like to Fight a National Security Letter

By Jennifer Valentino-DeVries

The saga of Nicholas Merrill's fight with the U.S. Justice Department began in 2004 with a strange phone call.



Bryan Thomas for The Wall Street Journal

Nicholas Merrill fought a national security letter after receiving one in 2004.

“They just said this is so-and-so from the FBI and we’re going to send somebody by with a letter,” says Mr. Merrill, the founder of a small New York Internet service provider called Calyx. I didn’t really take it seriously. I just said, ‘OK, that’s nice,’ and went back to my work.”

Then the FBI agent showed up at his office door. “The agent was wearing a trenchcoat and pulled out a huge wallet with a badge and then pulled out the letter,” Mr. Merrill says. “And then I realized it was serious.”

Mr. Merrill is one of only a few people in the U.S. who can talk publicly about what it’s like to



receive a national security letter, which allows the Federal Bureau of Investigation to seek financial, phone and Internet records about companies' customers.

The letters are the subject of [a story](#) in today's Wall Street Journal. Tens of thousands of them have been sent in previous years, but only a few people are known to have contested the letters or their associated gag orders.

Mr. Merrill went on to challenge the letter that he received, becoming the first person known to do so. Now, he is starting a telecommunications company dedicated to protecting its customers' privacy.

The letter that Mr. Merrill received in 2004 asked for a still-undisclosed list of information and instructed him that he could not tell anyone about the letter at all. Mr. Merrill didn't even know whether he could talk to his lawyer about it.

Later that year, in the U.S. District Court for the Southern District of New York, Judge Victor Marrero found that the law behind national security letters was unconstitutional, in part because it lacked a provision allowing for challenges.

Appeals and settlement negotiations continued in the case until 2010.

The FBI eventually dropped its request for information, but Mr. Merrill remained under the full secrecy order until the case was settled.

He said that during that time, he was unable to explain to people why he was missing important events or tell them when he was emotional about a ruling. During the trial, Mr. Merrill's father developed cancer; just before he died, Mr. Merrill says, he thought about telling him of the case, but eventually he decided against it.

"The gag order forced me to completely lie by omission or sometimes outright to the people closest to me," Mr. Merrill said. "I feel like if the FBI wants to put a gag on someone they should have to get permission from a judge."

His experience fighting the letter and the secrecy order have led him to found the [Calyx Institute](#), a non-profit that is "devoted to researching and implementing privacy technology and tools to promote free speech, free expression, civic engagement and privacy rights," according to its website.

He is now working to launch a for-profit subsidiary that will sell phone service that encodes the data running over it so that it is accessible only to the users and not to Calyx, the government or anyone else.

Calyx, like other resellers of mobile services, would have to run on another company's phone network. But the data itself would be encoded so that whoever is running the network would only have access to gibberish.

“As the service provider, we won’t be able to hand over anything besides encrypted data,” he says.

Such a service could present problems for law enforcement, which already has told lawmakers that it is “going dark” because of new technologies that aren’t required to give the government easy access for court-ordered surveillance.

Mr. Merrill has been hitting up venture capitalists and other donors in his quest to get \$2 million to launch the service later this year.

“What I’m trying to show is that there is a market for privacy,” he said.

As he does this, he says he plans to continue challenging the remaining part of the secrecy order. Although he has been able to talk about receiving the letter, he still isn’t allowed to say what the letter sought or who was targeted.

Copyright 2015 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit [www.djreprints.com](http://www.djreprints.com)

**EXHIBIT O**

The New York Times® Reprints

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers [here](#) or use the "Reprints" tool that appears next to any article. Visit [www.nytreprints.com](http://www.nytreprints.com) for samples and additional information. [Order a reprint of this article now.](#)

January 9, 2011

# Twitter Shines a Spotlight on Secret F.B.I. Subpoenas

By **NOAM COHEN**

THE news that federal prosecutors have demanded that the microblogging site [Twitter](#) provide the account details of people connected to the [WikiLeaks](#) case, including its founder, [Julian Assange](#), isn't noteworthy because the government's request was unusual or intrusive. It is noteworthy because it became public.

Even as Web sites, social networking services and telephone companies amass more and more information about their users, the government — in the course of conducting inquiries — has been able to look through much of the information without the knowledge of the people being investigated.

For the Twitter request, the government obtained a secret subpoena from a federal court. Twitter challenged the secrecy, not the subpoena itself, and won the right to inform the people whose records the government was seeking. WikiLeaks says it suspects that other large sites like [Google](#) and [Facebook](#) have received similar requests and simply went along with the government.

This kind of order is far more common than one may think, and in the case of terrorism and espionage investigations the government can issue them without a court order. The government says more than 50,000 of these requests, known as national security letters, are sent each year, but they come with gag orders that prevent those contacted from revealing what the agency has been seeking or even the existence of the gag orders.

“It’s a perfect example of how the government can use its broad powers to silence people,” said Nicholas Merrill, who was the first person to file a constitutional challenge against the use of national security letters, authorized by the [USA Patriot Act](#). Until August, he was forbidden to acknowledge the existence of a 2004 letter that the company he founded, the Calyx Internet Access Corporation, received from the [F.B.I.](#)

Mr. Merrill is now free to speak about the request, but part of the gag order remains in effect and he is still barred from discussing what information he had been asked to provide.



**MORE IN**  
**HBO S**  
**April.**

result, he said, before he gives a talk he consults a six-page guide prepared by his American Civil Liberties Union to be sure that he complies with the order to avoid punishment of five years in prison.

The government cites national security as the reason the contents of the letters — even their existence — are kept secret. The F.B.I. is trying to prevent plots as they are being hatched, according to Valerie Caproni, the general counsel of the agency, and thus needs stealth.

In the case of a small Internet service provider like Calyx, which was located in downtown Manhattan and had hundreds of customers, even mentioning that the F.B.I. had been sniffing around could harm an investigation, she said, especially if “the target is antsy anyway.”

Mr. Merrill, a 38-year-old from Brooklyn who studied computer science and philosophy, said he created Calyx in 1994 when it was “really pretty easy, there wasn’t really any competition.” His clients included “dozens of nonprofit organizations and alternative media outlets.”

Mr. Merrill challenged the constitutionality of the letter he received in 2004, saying the request raised “red flags” of being politically motivated. As a result of his suit and two later ones, the law governing the letters has been overturned and then revised by Congress.

In 2007, the F.B.I.’s inspector general found that the agency had abused its own guidelines by including too many peripheral people in its searches. The letters now receive the “individualized scrutiny” of the agents who are filing them, Ms. Caponi said.

All sides agree that it has become significantly easier to challenge the letters’ requests as well as their secrecy. At the moment, there are no new challenges in the court system, the government and the A.C.L.U. say.

The program, whose use has “ticked up” a bit in recent years, Ms. Caproni said, is humming along. She added, however, that the government had become more selective about the types of companies to which it sent letters. “All other things being the same, one of the things investigators think about is, ‘Who are we serving this? Are they comfortable with this?’ ” she said. “Most of these N.S.L.’s are filed on large companies. Why would they want to disclose that? Most companies view it as good corporate citizenry.”

One critic of the law, former Senator [Russ Feingold](#), said in a statement that it was long past time for Congress “to rein in the use of national security letters.”

“This is not a partisan issue,” Mr. Feingold said, “it is about the legislative branch providing an adequate check on the executive branch. Republicans advocating limited government should take a close look at these statutes and consider supporting changes.”

Mr. Merrill argues that the blanket gag orders have prevented a full public debate on the subject. He himself largely left the I.S.P. business in 2004, independent of his legal case, and only now has returned to hosting a couple of clients as part of a nonprofit project, the Calyx Institute, which aims to study how to protect consumers' privacy.

Regarding the news about Twitter, he wrote in an e-mail: "I commend Twitter's policy of notifying their customers of government requests for their private data and for their challenging and subsequently removing the gag order. This is a great example of the government's misuse of secrecy provisions and of exemplary privacy ethics on behalf of Twitter."

Ms. Caproni, who has testified before Congress about the program, said that it had been more than amply debated. "People at the A.C.L.U. and the press" think the letters are "a bigger deal than the companies."

To one of Mr. Merrill's A.C.L.U. lawyers, Jameel Jaffer, the smooth operation of the system is a sign that it is not working. The privacy rights at stake are not those of the companies who hold the information, Mr. Jaffer said, but "about people whose records are held." And those people should be told, he said.

"People used to be the custodians of their own records, their own diaries. Now third parties are custodians of all that," he said. "Everything you do online is entrusted to someone else — unless you want to go completely off the grid, and I'm not even sure that is possible."

**EXHIBIT P**

SUBSCRIBE

# ‘JOHN DOE’ WHO FOUGHT FBI SPYING FREED FROM GAG ORDER AFTER 6 YEARS



THE OWNER OF an internet service provider who mounted a high-profile court challenge to a secret FBI records demand has finally been partially released from a 6-year-old gag order that forced him to keep his role in the case a secret from even his closest friends and family. He can now identify himself and discuss the case, although he still can't reveal what information the FBI sought.

Nicholas Merrill, 37, was president of New York-based [Calvx Internet Access](#) when he received a so-called "national security letter" from the FBI in February 2004 demanding records of one of his customers and filed a lawsuit to challenge it. His company was a combination ISP and security consultancy business that was launched in the mid-90s and had about 200 customers, Merrill said, many of them advertising agencies and non-profit



groups.

Despite the fact that the FBI later dropped its demand for the records, Merrill was prohibited from telling his fiancée, friends or family members that he had received the letter or that he was embroiled in a lawsuit challenging its legitimacy. He occasionally showed up for court hearings about the case, but sat silently in the audience with other court observers. In 2007, he was prevented from publicly accepting an award for his courage from the American Civil Liberties Union, because he was not allowed to identify himself as the plaintiff in the case.

U.S. District Judge Victor Marrero in New York finally released Merrill partially from the gag order (.pdf) on July 30, which Merrill revealed publicly only on Monday.

“After six long years of not being able to tell anyone at all what happened to me – not even my family – I’m grateful to finally be able to talk about my experience of being served with a national security letter,” Merrill said in a statement. “Internet users do not give up their privacy rights when they log on, and the FBI should not have the power to secretly demand that ISPs turn over constitutionally protected information about their users without a court order. I hope my successful challenge to the FBI’s NSL gag power will empower others who may have received NSLs to speak out.”

A national security letter is an informal administrative letter the FBI can use to secretly demand customer records from ISPs, financial institutions, libraries, insurance companies, travel agencies, stockbrokers, car dealerships and others. NSLs have been used since the 1980s, but the Patriot Act, passed after the September 11, 2001 terrorist attacks, and a subsequent revision in 2003 expanded the kinds of records that could be obtained with an NSL.

With an NSL, the FBI does not need to seek a court order to obtain such records, nor does it need to prove just cause. An FBI field agent simply needs to draft an NSL stating the information being sought is “relevant” to a national security investigation.

The letters come with a life-long gag order, so businesses that receive such letters are prohibited from revealing to anyone, including customers who may be under investigation, that the government has requested records of transactions. Violation of a gag order can be punishable by up to five years in prison.

The gag orders raise the possibility for extensive abuse of NSLs, under the cover of secrecy. Indeed, in 2007, a Justice Department Inspector General audit found that the FBI, which issued almost 200,000 NSLs between 2003 and 2006, had abused its authority and misused NSLs.

In Merrill’s case, although the letter’s gag order “was totally clear that they were saying that I couldn’t speak to a lawyer” about it, he immediately contacted his personal attorney, and together they went to the ACLU in New York, which agreed to represent him.

“My gut feeling is I’m an American,” Merrill said, in an interview with Threat Level on Tuesday. “I always have a right to an attorney. There’s no such thing as you can’t talk to your attorney.

“I kind of felt at the beginning, so few people challenge this thing, I couldn’t just stand by and see, in my opinion, the basic underpinnings of our government undermined,” he continued. “I was taught about how sophisticated our system of checks and balances is . . . and if you really believe in that, then the idea of one branch of government just demanding records without being checked and balanced by the judicial just is so obviously wrong on the surface.”

Merrill and the ACLU filed the lawsuit under the name “John Doe,” challenging the legality of the letter and asserting that customer records

were constitutionally protected information. Merrill said the NSL, which listed 16 categories of records, including e-mail and billing records, was “very broad.”

“It was kind of open ended,” he said. “It went through a list of things and then said ‘and anything else.’ The implication was just send us everything and the kitchen sink.”

Merrill wouldn’t say how many records he had that were relevant to the request but said in general, “In the most broad understanding of what is electronic communication transaction records, I probably had like thousands and thousands of records on each client, if you consider that you host things and you’re using software that creates log files. . . . ISPs have a lot of records on every client typically. They may have records of every time you posted something, of every web site you visited.”

Over the years the case progressed, Merrill was careful not to disclose his identity. At one point he attended a packed hearing — filled with law school students and media — but he was careful not to speak with anyone.

Friends began to question whether he was John Doe when he was publicly identified with a second case involving a grand iury subpoena from the Secret Service for customer records related to the news site IndyMedia. In that case, no gag order was imposed. Merrill said he was forced to lie when asked about John Doe or simply refused to answer.

“It put me in a very difficult position,” he said.

In 2007, the ACLU granted “John Doe” a liberty award, along with four Connecticut librarians who also filed a legal challenge over NSLs. Because of the gag order against Merrill, the ACLU had to present his award to an empty chair.

In December 2008, the Second Circuit Court of Appeals ruled that some of the NSL gag provisions were unconstitutional, in part because they limited judicial review of the gag orders and forced courts to defer to the government's assertions about the necessity of a gag order and also thwarted the ability of recipients to challenge a gag order. The case was sent back to the U.S. District Court for the Southern District of New York, forcing the government to justify the constitutionality of the gag order imposed on Merrill.

In June 2009, the government introduced secret evidence to the court to justify continuing the gag order, claiming that if information were revealed about the letter it would harm an ongoing investigation. Merrill and his attorneys were prevented from learning the specifics of the evidence in order to refute it. The government was then ordered by the court to produce an unclassified summary of its evidence.

The ACLU worked hard to negotiate a partial gag-lift with the government that allowed Merrill to finally identify himself, while still keeping the details of the letter secret. In return, Merrill and the ACLU agreed to drop their appeal of the case.

Although the case helped expose the secrecy around NSLs and resulted in some First Amendment progress for entities receiving such requests — Congress amended the law to allow recipients to challenge NSLs and gag orders, and the FBI must now also prove in court that disclosure of an NSL would harm a national security case — the fight over NSLs is not over. The Obama administration has been seeking to expand the FBI's power to demand internet activity records of customers without court approval or suspicion of wrongdoing. If granted, the data sought without a court order could expand to include web browser and search history, and Facebook friend requests.

“Even though this case has resulted in significant improvements to NSL procedures, innocent Americans' private records remain too vulnerable to

secret and warrantless data collection by the FBI,” said Melissa Goodman, staff attorney with the ACLU National Security Project in a statement. “At a minimum, the FBI should have to show individual suspicion before it issues an NSL for an individual’s personal information and invades Americans’ right to privacy and free speech on the Internet.”

The FBI’s use of national security letters to get information on Americans without a court order increased from 16,804 in 2007 to 24,744 in 2008. The 2008 requests targeted 7,225 U.S. people.

In the 2007 inspector general’s report, investigators found that the FBI had failed to adequately justify some letters, had evaded limits on (and sometimes illegally issued) NSLs to obtain phone, e-mail and financial information on American citizens, and had under-reported the use of NSLs to Congress.

About 60 percent of a sample of the FBI’s NSLs did not conform to Justice Department rules, and another 22 percent possibly violated the statute because they made improper requests of businesses or involved unauthorized collections of information.

Subsequently, the number of NSLs issued in 2007 dramatically dropped from 49,000 to 16,000, but has rebounded in recent years.

Merrill’s experience with the case has prompted him to launch a non-profit, the [Calvx Institute](#), aimed at educating the technology and telecommunications industry and developing best practices and tools for safeguarding the privacy of customers.

“I feel there’s a lot of work to be done,” he said. “The case has made me realize that just one or two people standing up can have a great effect. I either want to inspire others to follow the example . . . or develop technology that makes it more difficult for people to be snooped on.”

*Photo: ACLU*

# **EXHIBIT Q**

---

# LIBERTY AND SECURITY IN A CHANGING WORLD

---

12 December 2013

**Report and Recommendations of  
The President's Review Group on Intelligence  
and Communications Technologies**

**[ Pages for Transmittal Letter and Acknowledgments omitted ]**



## **Table of Contents**

### **Preface**

### **Executive Summary**

### **Recommendations**

### **Chapter I: Principles**

### **Chapter II: Lessons of History**

- A. The Continuing Challenge
- B. The Legal Framework as of September 11, 2001
- C. September 11 and its Aftermath
- D. The Intelligence Community

### **Chapter III: Reforming Foreign Intelligence Surveillance Directed at United States Persons**

- A. Introduction
- B. Section 215: Background
- C. Section 215 and “Ordinary” Business Records

- D. National Security Letters
- E. Section 215 and the Bulk Collection of Telephony Meta-data
  - 1. The Program
  - 2. The Mass Collection of Personal Information
  - 3. Is Meta-data Different?
- F. Secrecy and Transparency

#### **Chapter IV: Reforming Foreign Intelligence Surveillance Directed at Non-United States Persons**

- A. Introduction
- B. Foreign Intelligence Surveillance and Section 702
- C. Privacy Protections for United States Persons Whose Communications are Intercepted Under Section 702
- D. Privacy Protections for Non-United States Persons

#### **Chapter V: Determining What Intelligence Should Be Collected and How**

- A. Priorities and Appropriateness
- B. Monitoring Sensitive Collection
- C. Leadership Intentions

D. Cooperation with Our Allies

**Chapter VI: Organizational Reform in Light of Changing Communications Technology**

A. Introduction

B. The National Security Agency

1. “Dual-Use” Technologies: The Convergence of Civilian Communications and Intelligence Collection

2. Specific Organizational Reforms

C. Reforming Organizations Dedicated to the Protection of Privacy and Civil Liberties

D. Reforming the FISA Court

**Chapter VII: Global Communications Technology: Promoting Prosperity, Security, and Openness in a Networked World**

A. Introduction

B. Background: Trade, Internet Freedom, and Other Goals

1. International Trade and Economic Growth

2. Internet Freedom

3. Internet Governance and Localization Requirements
- C. Technical Measures to Increase Security and User Confidence
- D. Institutional Measures for Cyberspace
- E. Addressing Future Technological Challenges

## **Chapter VIII. Protecting What We Do Collect**

- A. Personnel Vetting and Security Clearances
  1. How the System Works Now
  2. How the System Might be Improved
  3. Information Sharing
- B. Network Security
  1. Executive Order 13578
  2. Physical and Logical Separation
- C. Cost-Benefit Analysis and Risk Management

## **Conclusion**

**Appendix A:** The Legal Standards for Government Access to Communications

**Appendix B:** Overview of NSA Privacy Protections Under FAA 702

Overview of NSA Privacy Protections Under EO 12333

**Appendix C:** US Intelligence: Multiple Layers of Rules and Oversight

**Appendix D:** Avenues for Whistle-blowers in the Intelligence  
Community

**Appendix E:** US Government Role in Current Encryption Standards

**Appendix F:** Review Group Briefings and Meetings

**Appendix G:** Glossary

**[ Pages 10 - 88 omitted ]**

any *particular* individual or organization. The requirement of an explicit judicial finding that the order is “reasonable in focus, scope, and breadth” is designed to ensure this critical element of judicial oversight.

#### **D. National Security Letters**

##### **Recommendation 2**

**We recommend that statutes that authorize the issuance of National Security Letters should be amended to permit the issuance of National Security Letters only upon a judicial finding that:**

- (1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect “against international terrorism or clandestine intelligence activities” and**
- (2) like a subpoena, the order is reasonable in focus, scope, and breadth.**

##### **Recommendation 3**

**We recommend that all statutes authorizing the use of National Security Letters should be amended to require the use of the same oversight, minimization, retention, and dissemination standards that currently govern the use of section 215 orders.**

Shortly after the decision in *Miller*, Congress created the National Security Letter (NSL) as a form of administrative subpoena.<sup>71</sup> NSLs, which

---

<sup>71</sup> Administrative subpoenas are authorized by many federal statutes and may be issued by most federal agencies. Most statutes authorizing administrative subpoenas authorize an agency to require the production of certain records for civil rather than criminal matters.

are authorized by five separate federal statutory provisions,<sup>72</sup> empower the FBI and other government agencies in limited circumstances to compel individuals and organizations to turn over to the FBI in the course of national security investigations many of the same records that are covered by section 215 and that criminal prosecutors can obtain through subpoenas issued by a judge or by a prosecutor in the context of a grand jury investigation. NSLs are used primarily to obtain telephone toll records, e-mail subscriber information, and banking and credit card records. Although NSLs were initially used sparingly, the FBI issued 21,000 NSLs in Fiscal Year 2012, primarily for subscriber information. NSLs are most often used early in an investigation to gather information that might link suspected terrorists or spies to each other or to a foreign power or terrorist organization.

When NSLs were first created, the FBI was empowered to issue an NSL only if it was authorized by an official with the rank of Deputy Assistant Director or higher in the Bureau's headquarters, and only if that official certified that there were "specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or an agent of a foreign power."<sup>73</sup> The PATRIOT Act of 2001 significantly expanded the FBI's authority to issue NSLs. First, the PATRIOT Act authorized every Special Agent in Charge of any of the Bureau's 56 field offices around the country to issue NSLs. NSLs therefore no longer have to be issued by high-level officials at FBI headquarters.

---

<sup>72</sup> 12 U.S.C. § 3414, 15 U.S.C. § 1681(u), 15 U.S.C. § 1681(v), 18 U.S.C. § 2709, and 50 U.S.C. § 436.

<sup>73</sup> 50 U.S.C. § 1801.



Second, the PATRIOT Act eliminated the need for any *particularized* showing of individualized suspicion.<sup>74</sup> Under the PATRIOT Act, the FBI can issue an NSL whenever an authorized FBI official certifies that the records sought are “relevant to an authorized investigation.” Third, the PATRIOT Act empowered the FBI to issue nondisclosure orders (sometimes referred to as “gag orders”) that prohibit individuals and institutions served with NSLs from disclosing that fact, and it provided for the first time for judicial enforcement of those nondisclosure orders.<sup>75</sup> In contemplating the power granted to the FBI in the use of NSLs, it is important to emphasize that NSLs are issued directly by the FBI itself, rather than by a judge or by a prosecutor acting under the auspices of a grand jury.<sup>76</sup> Courts ordinarily enter the picture only if the recipient of an NSL affirmatively challenges its legality.<sup>77</sup>

NSLs have been highly controversial. This is so for several reasons. First, as already noted, NSLs are issued by FBI officials rather than by a judge or by a prosecutor in the context of a grand jury investigation. Second, as noted, the standard the FBI must meet for issuing NSLs is very low. Third, there have been serious compliance issues in the use of NSLs. In 2007, the Department of Justice’s Office of the Inspector General detailed

---

<sup>74</sup> Pub. L. 107-56, 115 Stat. 365 (2001).

<sup>75</sup> See 18 U.S.C. § 3511.

<sup>76</sup> It should be noted that there are at least two distinctions between NSLs and federal grand jury subpoenas. First, where the FBI believes that records should be sought, it can act directly by issuing NSLs, but to obtain a grand jury subpoena the FBI must obtain approval by a prosecutor at the Department of Justice. Second, and except in exceptional circumstances, witnesses who appear before a grand jury ordinarily are not under nondisclosure orders preventing them from stating that they have been called as witnesses.

<sup>77</sup> See David S. Kris and J. Douglas Wilson, *1 National Security Investigations and Prosecutions 2d*, pp. 727-763 (West 2012).

extensive misuse of the NSL authority, including the issuance of NSLs without the approval of a properly designated official and the use of NSLs in investigations for which they had not been authorized.<sup>78</sup> Moreover, in 2008, the Inspector General disclosed that the FBI had “issued [NSLs] . . . after the FISA Court, citing First Amendment concerns, had twice declined to sign Section 215 orders in the same investigation.”<sup>79</sup> Fourth, the oversight and minimization requirements governing the use of NSLs are much less rigorous than those imposed in the use of section 215 orders.<sup>80</sup> Fifth, nondisclosure orders, which are used with 97 percent of all NSLs, interfere with individual freedom and with First Amendment rights.<sup>81</sup>

There is one final—and important— issue about NSLs. For all the well-established reasons for requiring neutral and detached judges to decide when government investigators may invade an individual’s privacy, there is a strong argument that NSLs should not be issued by the FBI itself. Although administrative subpoenas are often issued by administrative agencies, foreign intelligence investigations are especially likely to implicate highly sensitive and personal information and to have potentially severe consequences for the individuals under investigation.

---

<sup>78</sup> See Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation’s Use of National Security Letters (Unclassified)* (March 2007). *Note: Subsequent reports from the IG have noted the FBI and DOJ have resolved many of the compliance incidents.*

<sup>79</sup> United States Department of Justice, Office of the Inspector General, *A Review of the FBI’s Use of Section 215 Orders for Business Records in 2006* 5 (March 2008), quoted in Kris & Wilson, *National Security Investigations and Prosecutions* at 748. In recent years, the FBI has put in place procedures to reduce the risk of noncompliance.

<sup>80</sup> 18 U.S.C. § 1861(g).

<sup>81</sup> In *Doe v. Mukasey*, 549 F.3d 861 (2d Cir. 2008), the court held that the FBI’s use of nondisclosure orders violated the First Amendment. In response, the FBI amended its procedures to provide that if a recipient of an NSL objects to a non-disclosure order, the FBI must obtain a court order based on a demonstrated need for secrecy in order for it to enforce the non-disclosure order.

We are unable to identify a principled reason why NSLs should be issued by FBI officials when section 215 orders and orders for pen register and trap-and-trace surveillance must be issued by the FISC.

We recognize, however, that there are legitimate practical and logistical concerns. At the current time, a requirement that NSLs must be approved by the FISC would pose a serious logistical challenge. The FISC has only a small number of judges and the FBI currently issues an average of nearly 60 NSLs per day. It is not realistic to expect the FISC, as currently constituted, to handle that burden. This is a matter that merits further study. Several solutions may be possible, including a significant expansion in the number of FISC judges, the creation within the FISC of several federal magistrate judges to handle NSL requests, and use of the Classified Information Procedures Act<sup>82</sup> to enable other federal courts to issue NSLs.

We recognize that the transition to this procedure will take some time, planning, and resources, and that it would represent a significant change from the current system. We are not suggesting that the change must be undertaken immediately and without careful consideration. But it should take place as soon as reasonably possible. Once the transition is complete, NSLs should not issue without prior judicial approval, in the absence of an emergency where time is of the essence.<sup>83</sup> We emphasize the importance of the last point: In the face of a genuine emergency, prior

---

<sup>82</sup> 18 U.S.C. app. 3 §§ 1-16.

<sup>83</sup> It is essential that the standards and processes for issuance of NSLs match as closely as possible the standards and processes for issuance of section 215 orders. Otherwise, the FBI will naturally opt to use NSLs whenever possible in order to circumvent the more demanding – and perfectly appropriate – section 215 standards. We reiterate that if judicial orders are required for the issuance of NSLs, there should be an exception for emergency situations when time is of the essence.

**[ Pages 94 - 121 omitted ]**

## F. Secrecy and Transparency

### Recommendation 7

We recommend that legislation should be enacted requiring that detailed information about authorities such as those involving National Security Letters, section 215 business records, section 702, pen register and trap-and-trace, and the section 215 bulk telephony meta-data program should be made available on a regular basis to Congress and the American people to the greatest extent possible, consistent with the need to protect classified information. With respect to authorities and programs whose existence is unclassified, there should be a strong presumption of transparency to enable the American people and their elected representatives independently to assess the merits of the programs for themselves.

### Recommendation 8

We recommend that:

- (1) legislation should be enacted providing that, in the use of National Security Letters, section 215 orders, pen register and trap-and-trace orders, 702 orders, and similar orders directing individuals, businesses, or other institutions to turn over information to the government, non-disclosure orders may be issued only upon a judicial finding that there are reasonable grounds to believe that disclosure would significantly threaten the national security, interfere with an ongoing investigation, endanger the life or physical safety of any person, impair

diplomatic relations, or put at risk some other similarly weighty government or foreign intelligence interest;

- (2) nondisclosure orders should remain in effect for no longer than 180 days without judicial re-approval; and
- (3) nondisclosure orders should never be issued in a manner that prevents the recipient of the order from seeking legal counsel in order to challenge the order's legality.

#### Recommendation 9

We recommend that legislation should be enacted providing that, even when nondisclosure orders are appropriate, recipients of National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders issued in programs whose existence is unclassified may publicly disclose on a periodic basis general information about the number of such orders they have received, the number they have complied with, the general categories of information they have produced, and the number of users whose information they have produced in each category, unless the government makes a compelling demonstration that such disclosures would endanger the national security.

#### Recommendation 10

We recommend that, building on current law, the government should publicly disclose on a regular basis general data about National Security Letters, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders in programs whose

existence is unclassified, unless the government makes a compelling demonstration that such disclosures would endanger the national security.

### Recommendation 11

We recommend that the decision to keep secret from the American people programs of the magnitude of the section 215 bulk telephony meta-data program should be made only after careful deliberation at high levels of government and only with due consideration of and respect for the strong presumption of transparency that is central to democratic governance. A program of this magnitude should be kept secret from the American people only if (a) the program serves a compelling governmental interest and (b) the efficacy of the program would be *substantially* impaired if our enemies were to know of its existence.

A free people can govern themselves only if they have access to the information that they need to make wise judgments about public policy. A government that unnecessarily shields its policies and decisions from public scrutiny therefore undermines the most central premise of a free and self-governing society. As James Madison observed, “A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both.”<sup>122</sup>

There is no doubt that in the realm of national security, the nation needs to keep secrets. The question, though, is what information must be

---

<sup>122</sup> Letter from James Madison to W.T. Barry (Aug. 4, 1822) in *The Writings of James Madison* at 103 (Gaillard Hunt, ed., G.P. Putnam’s Sons) 1910.

kept secret. The reasons why government officials want secrecy are many and varied. They range from the truly compelling to the patently illegitimate. Sometimes government officials want secrecy because they rightly fear that the disclosure of certain information might seriously undermine the nation's security. Sometimes they want secrecy because they do not want to have to deal with public criticism of their decisions or because they do not want the public, Congress, or the courts to override their decisions, which they believe to be wise. Sometimes they want secrecy because disclosure will expose their own incompetence, noncompliance, or wrongdoing. Some of those reasons for secrecy are obviously more worthy of deference than others.

Adding to the complexity, the contribution of any particular disclosure to informed public discourse may vary widely depending upon the nature of the information. The disclosure of some confidential information may be extremely valuable to public debate (for example, the revelation of unwise or even unlawful government programs). The disclosure of other confidential information, however, may be of little or no legitimate value to public debate (for example, publication of the identities of covert American agents). The most vexing problems arise when the public disclosure of secret information is *both* harmful to national security *and* valuable to informed self-governance.

There is a compelling need today for a serious and comprehensive reexamination of the balance between secrecy and transparency. In considering this question, the Public Interest Declassification Board (PIDB)



recently observed: “A Democratic society is grounded in the informed participation of the citizenry, and their informed participation requires access to Government information. An open record of official decisions is essential to educate and inform the public and enable it to assess the policies of its elected leaders. If officials are to be accountable for their actions and decisions, secrecy must be kept to the minimum required to meet legitimate national security considerations. . . . Better access to Government records and internal history will help both policymakers and the American public meet their mutual responsibilities to address national security and foreign policy challenges consistent with democratic values.” The PIDB concluded that it is necessary for the United States to make the reforms necessary “to transform current classification and declassification guidance and practice.”<sup>123</sup>

Another dimension to the secrecy vs. transparency issue concerns the role of whistle-blowers. Although an individual government employee or contractor should not take it upon himself to decide on his own to “leak” classified information because he thinks it would be better for the nation for the information to be disclosed, it is also the case that a free and democratic nation needs safe, reliable, and fair-minded processes to enable such individuals to present their concerns to responsible and independent officials. After all, their concerns might be justified. It does not serve the nation for our government to prevent information that should be disclosed from being disclosed. Although such mechanisms exist, they can certainly

---

<sup>123</sup> Public Interest Declassification Board, *Transforming the Security Classification System*, 1-2 (2012), pp.1-2.

be strengthened and made more accessible.<sup>124</sup> Appendix D sets forth existing mechanisms for whistle-blowing.

The secrecy vs. transparency issue also has serious repercussions today for the freedom of the press. It is the responsibility of our free press to expose abuse, over-reaching, waste, undue influence, corruption, and bad judgment on the part of our elected officials. A robust and fearless freedom of the press is essential to a flourishing self-governing society. It will not do for the press to be fearful, intimidated, or cowed by government officials. If they are, it is “We the People” who will suffer. Part of the responsibility of our free press is to ferret out and expose information that government officials would prefer to keep secret when such secrecy is unwarranted. This point raises fundamental issues about press shield laws, spying on members of the press and their sources, investigating members of the press, and attempting to intimidate members of the press.

At the same time, the potential danger of leaks is more serious than ever, especially in light of the fact that information can be spread instantly across the globe. The fact that classified information can now be stolen, either by insiders or outsiders, in massive quantities, creates

---

<sup>124</sup> On October 10, 2012, President Obama issued Presidential Policy Directive/PPD-19, which prohibits any retaliatory employment action against any government employee with access to classified information who reports any instance of “waste, fraud, and abuse,” including violations “of any law, rule, or regulation,” to “a supervisor in the employee’s direct chain of command up to and including the head of the employing agency, to the Inspector General of the employing agency or Intelligence Community Element, to the Director of National Intelligence, to the Inspector General of the Intelligence Community.” *Id.* Although this is an important step in the right direction, it does not go far enough. First, it covers only government employees and not government contractors. Second, it requires the would-be whistle-blower to report to a person in his “direct chain of command,” rather than to an independent authority. We discuss whistle-blowing in Chapter VI.

unprecedented dangers. Put simply, the stakes on both sides—national security and effective self-governance—are high.

At the very least, we should always be prepared to question claims that secrecy is necessary. That conclusion needs to be demonstrated rather than merely assumed. When it is possible to promote transparency without appreciably sacrificing important competing interests, we should err on the side of transparency.

Thus, in implementing NSLs, section 215 orders, pen register and trap-and-trace orders, section 702 orders, and similar orders in programs whose existence is unclassified, the government should, to the greatest extent possible, report publicly on the total number of requests made and the number of individuals whose records have been requested. These totals inform Congress and the public about the overall size and trends in a program, and are especially informative when there are major changes in the scale of a program. In addition, providers have shown a strong interest in providing periodic transparency reports about the number of requests to which they have responded. Reports from providers can be a useful supplement to reports from the government—the existence of multiple sources of information reduces the risk of inaccurate reporting by any one source. Reports from providers are also an important way for providers to assure customers and the general public that they are careful stewards of their users' records. As discussed in Chapter VII, such transparency reports from providers should be permitted and encouraged by governments throughout the world, and the US Government should work with allies to

enable accurate reporting about government requests in other countries as well as in the United States.

In some instances, over-reporting can also be a problem. This might occur when there are duplicative reports, which burden agencies with redundant requirements. To address this concern, the government should catalog the current reporting requirements on FISA, NSLs, and other intelligence-related statistics, and document how frequently these reports are made and to whom. As shown in Appendix C, multiple oversight mechanisms exist for reporting to Congress and within the Executive Branch. A catalog of existing reports would create a more informed basis for deciding what changes in reporting might be appropriate. Moreover, in some instances public reports can unintentionally harm the national security by inadvertently revealing critical information. For instance, detailed reports by small Internet service providers about government requests for information might inadvertently tip off terrorists or others who are properly under surveillance. To reduce this risk, reporting requirements should be less detailed in those situations in which reporting about a small number events might reveal critical information to those under surveillance.<sup>125</sup>

---

<sup>125</sup> Similarly, in the context of the non-disclosure orders addressed in Recommendation 9, the government should be able to act without prior judicial authority in cases of emergency.

**[ Pages 130 - 304 omitted ]**

# **EXHIBIT R**

Nos. 13-15957 and 13-16731

**UNDER SEAL**

---

IN THE UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT

---

UNDER SEAL,

Petitioner-Appellee (No. 13-15957),

Petitioner-Appellant (No. 13-16731),

v.

ERIC H. HOLDER, JR., ATTORNEY GENERAL; UNITED STATES  
DEPARTMENT OF JUSTICE; and FEDERAL BUREAU OF INVESTIGATION,

Respondents-Appellants (No. 13-15957),

Respondents-Appellees (No. 13-16731).

---

On Appeal from the United States District Court  
for the Northern District of California  
Case No's. 11-cv-2173 SI & 13-mc-80089 SI  
Honorable Susan Illston, District Court Judge

---

**BRIEF *AMICI CURIAE* OF EXPERTS IN COMPUTER SCIENCE  
AND DATA SCIENCE IN SUPPORT OF APPELLANTS**

---

Phillip R. Malone, CA Bar No. 163969  
Michael Chen, CA Bar Student Cert. No. 34469  
Emily Warren, CA Bar Student Cert. No. 34473  
Rachel Yu, CA Bar Student Cert. No. 34474  
JUELSGAARD INTELLECTUAL  
PROPERTY & INNOVATION CLINIC  
Mills Legal Clinic at Stanford Law School  
559 Nathan Abbott Way  
Stanford, California 94305-8610  
Telephone: (650) 725-6369

*Counsel for Amici Curiae*

## **CORPORATE DISCLOSURE STATEMENT**

Pursuant to Federal Rule of Appellate Procedure 26.1, each of the amici listed in Exhibit A states that he or she is not a corporation that issues stock and has no parent corporation.



**TABLE OF CONTENTS**

STATEMENT OF INTEREST ..... 1

INTRODUCTION ..... 2

ARGUMENT ..... 3

    I.    NATIONAL SECURITY LETTERS GIVE THE FBI  
        EXTENSIVE AUTHORITY TO SURVEIL ORDINARY  
        AMERICANS ..... 3

    II.   NSL DATA REVEAL DEEPLY SENSITIVE  
        INFORMATION ABOUT INDIVIDUALS AND THEIR  
        ASSOCIATIONS ..... 15

        A.   Even a Single Call, Text, or E-mail Reveals Sensitive  
            Information..... 17

        B.   Patterns of Calls, Texts, and Emails Reveal Even More  
            Sensitive Information..... 22

            1.   Social Graph and Predictive Modeling Techniques  
                are Easy to Implement and Immensely Informative ..... 23

            2.   NSL Data Reveal Extensive Private Political,  
                Personal, Associational, Religious, Corporate,  
                Medical, and Financial Information ..... 27

CONCLUSION ..... 33

STATEMENT OF RELATED CASES ..... 34

CERTIFICATE OF COMPLIANCE ..... 35

**TABLE OF AUTHORITIES**

**Cases**

*ACLU v. Clapper*, 33-cv-03994 (WHP) (SDN& Aug. 23, 2013) Dkt 27,  
 Declaration of Edward W. Felton.....21, 28

**Statutes**

Electronic Communications Privacy Act (ECPA).....passim

18 U.S.C. § 2510(8) .....5

18 U.S.C. § 2703(c)(1).....7

18 U.S.C. § 2709 .....14,15

18 U.S.C. § 2709(a)-(b) .....2, 3, 4

50 U.S.C. § 1861 .....7

**Agency Publications, Reports and Opinions**

*Administration White Paper: Bulk Collection of Telephony Metadata Under  
 Section 215 of the USA Patriot Act 2* (Aug. 9, 2013).....7, 16

Daniel Koffsky, *Requests for Information Under the Electronic  
 Communications Privacy Act, in 32 Opinions of the Office of Legal  
 Counsel* (2008).....4

The President’s Review Group on Intelligence and Communications  
 Technologies, *Final Report 90* (2013).....4, 6, 7, 8

State of California Franchise Tax Board, *Reporting Income Tax Fraud*,  
[https://www.ftb.ca.gov/online/Fraud\\_Referral/important\\_information.asp](https://www.ftb.ca.gov/online/Fraud_Referral/important_information.asp)..... 18

U.S. Department of Justice Office of the Inspector General, *A Review of the  
 FBI’s Use of National Security Letters: Assessment of Corrective Actions  
 and Examination of NSL Usage in 2006* (2008).....7, 8, 10, 15

U.S. Department of Justice Office of the Inspector General, *A Review of the  
 FBI’s Use of Section 215 Orders for Business Records in 2006 5* (2008).....14

U.S. Department of Justice Office of the Inspector General, *A Review of the FBI’s Use of National Security Letters* 36 (2007).....passim

U.S. Department of Justice Office of the Inspector General, *A Review of the Federal Bureau of Investigation’s Use of Exigent Letters and Other Informal Requests for Telephone Records* 75 (2010).....11, 14, 15

**Magazines, Newspapers and Blogs**

Matt Blaze, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)*, *Wired* (June 16, 2013 9:30 AM), <http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again> .....16, 27

The Economist, *Mining Social Networks: Untangling the Social Web*, (Sept. 2, 2010), <http://www.economist.com/node/16910031> .....30

Dan Eggen, *Text ‘Give’ to Obama: President’s Campaign Launches Cellphone Donation Drive*, *Wash. Post* (Aug. 23, 2012), [http://www.washingtonpost.com/politics/text-give-to-obama-presidents-campaign-launches-cellphone-donation-drive/2012/08/23/5459649a-ecc4-11e1-9ddc-340d5efb1e9c\\_story.html](http://www.washingtonpost.com/politics/text-give-to-obama-presidents-campaign-launches-cellphone-donation-drive/2012/08/23/5459649a-ecc4-11e1-9ddc-340d5efb1e9c_story.html) .....22

Barton Gellman, *NSA Statements to the Post*, *Wash. Post*, Aug 15, 2013, <http://wapo.st/1ixchnm> .....18

Hal Hodson, *How Metadata Brought Down CIA Boss David Petraeus*, *NewsScientist* (Nov. 16, 2013 1:59 PM), <http://www.newscientist.com/article/dn22511-how-metadata-brought-down-cia-boss-david-petraeus.html>.....29

Mail & Guardian, *Story Tip-Offs*, <http://mg.co.za/page/story-tip-offs> .....19

Jane Mayer, *What’s the Matter With Metadata?*, *New Yorker* (June 6, 2013), <http://www.newyorker.com/online/blogs/newsdesk/2013/06/verizon-nsa-metadata-surveillance-problem.html> .....6, 16, 28, 32

New York Times, *Contact the Public Editor*, *NYTimes.com*, <http://publiceditor.blogs.nytimes.com/contact-the-public-editor/> .....18

Rebecca J. Rosen, *Stanford Researchers: It is Trivially Easy to Match Metadata to Real People*, *The Atlantic* (Dec. 24, 2013 1:50 PM), <http://www.theatlantic.com/technology/archive/2013/12/stanford-researchers-it-is-trivially-easy-to-match-metadata-to-real-people/282642> ..... 17

**Internet Sources**

Griffin Boyce and Brian Duggan, *The Real Reason Why Metadata Collecting Is Dangerous*, *New America Foundation* (June 17, 2013 4:54 PM), <http://inthe tank.newamerica.net/blog/2013/06/real-reason-why-metadata-collecting-dangerous> ..... 21

Childhelp, *Childhelp National Child Abuse Hotline*, <http://childhelp.org/pages/hotline-home> ..... 18

Charles Duhigg, *How Companies Learn Your Secrets* (Feb. 16, 2012), [http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&\\_r=1&hp](http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp) ..... 33

Electronic Privacy Information Center, *National Security Letters*, <http://epic.org/privacy/nsl/> ..... 4

GLBT National Help Center, *Gay, Lesbian, Bisexual and Transgender National Hotline*, <http://www.glbtnationalhelpcenter.org/hotline> ..... 18

IBM, *Analyst’s Notebook*, <http://www-03.ibm.com/software/products/en/analysts-notebook-family> ..... 26

IBM, *Environmental Investigation Agency: IBM i2 Solution Help Combat the Illegal Tiger Trade* (2012) ..... 26

Jonathan Mayer & Patrick Mutchler, *MetaPhone: The NSA Three-Hop, Web Policy* (Dec. 9, 2013), <http://webpolicy.org/2013/12/09/metaphone-the-nsa-three-hop/> ..... 13, 14, 18

Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, *Web Policy* (Mar. 12, 2014), <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata> ..... 18, 20, 30, 33

MIT Media Lab, *Immersion*, <https://immersion.media.mit.edu> ..... 25

Chris Soghoian, *US Surveillance Law May Poorly Protect New Text Message Services*, American Civil Liberties Union (Jan. 8, 2013, 9:44 AM), <https://www.aclu.org/blog/national-security-technology-and-liberty/us-surveillance-law-may-poorly-protect-new-text> ..... 5

Susan G. Komen for the Cure, *Donate by Text*, <http://www5.komen.org>..... 223

Pete Yost & Matt Apuzzo, *With 3 ‘Hops,’ NSA Gets Millions of Phone Records*, Associated Press (Jul. 31, 2013 6:19 PM), <http://bigstory.ap.org/article/senate-panel-looking-limits-surveillance> ..... 11

## STATEMENT OF INTEREST<sup>1</sup>

The amici listed in Exhibit A are professors of computer and data science at the country's leading educational institutions, and expert computer scientists, specializing in data and computer security, data analysis, cryptography, and privacy-enhancing technologies. Collectively, amici's research has significantly shaped the development of modern communications technology and data analysis techniques.

Amici offer this brief to emphasize for the Court the extraordinary sensitivity of the data that can be gathered through National Security Letters, notwithstanding its legal categorization as "non-content" data, and the personal, intimate, family, associational, political, health and medical, financial and other information that can be revealed by such data. Amici's expertise and familiarity with data analysis and communications technology offer a particularly informed perspective on the issues confronted in this case. The list of amici attached as Exhibit A includes a brief biography of each.

---

<sup>1</sup> Pursuant to Federal Rule of Appellate Procedure 29(c)(5), no one, except for the amici and their counsel, has authored this brief in whole or in part, or contributed money towards its preparation. All parties have consented to the filing of this brief.

## INTRODUCTION

Under the Electronic Communications Privacy Act (ECPA) National Security Letter (NSL) provisions of 18 U.S.C. § 2709(a)-(b), the FBI easily surveils ordinary Americans. NSLs can be obtained merely with the signature of any special agent in charge of any FBI field office, and there is no need for suspicion of wrongdoing. The data seized need only be considered “relevant” to a counterintelligence or counterterrorism investigation, and the person whose data are taken need not be in any way considered a suspect or target.

With no affirmative judicial approval of the NSL process and a low “relevance” standard that encompasses potentially millions of people per single NSL request, the government unreasonably invades the privacy of potentially every American. Through the hundreds of thousands of NSLs have already been issued, the FBI may have collected data on almost every person in the United States. And once collected, NSL data typically is stored in massive databases and can be accessed broadly—not just by top FBI officials.

While the government asserts that the information obtained by NSLs does not include the actual content of a communication, NSL information can nonetheless be incredibly revealing. Through even a relatively naïve analysis of information obtained by an NSL, the FBI can gather extensive information about a person’s political contributions, intimate relationships, religious and community

affiliations, medical conditions, financial records, and much more. The rise of “Big Data” and sophisticated analytical tools only compound this danger, giving the government unprecedented access to the sensitive information of American citizens.

## **ARGUMENT**

### **I. NATIONAL SECURITY LETTERS GIVE THE FBI EXTENSIVE AUTHORITY TO SURVEIL ORDINARY AMERICANS**

The current version of the substantive ECPA NSL provisions, codified at 18 U.S.C. § 2709(a)-(b), authorizes dozens of FBI agents around the country to issue national security letters without meaningful, affirmative judicial checks. These letters can compel the disclosure of all non-content data connected with phone calls, text messages, and emails—essentially, everything except for actual recordings and copies of the messages themselves. Agents can collect data pertaining to any entity that may be “relevant” to an investigation and have issued hundreds of thousands of requests for such data. Moreover, since “relevant” may be defined however the Bureau wishes, the standard offers it great discretion to collect data on nearly any American. Once collected, these data are stored in databases accessible by tens of thousands of people and are used to produce intelligence reports for dozens of agencies. Predictably but unfortunately, there is



substantial evidence that the FBI has abused these expansive authorities.<sup>2</sup>

Though the type of data that the FBI may demand under § 2709(a)-(b) has not been fully litigated, public and private actors have interpreted the statute's key terms (subscriber information, toll billing records, and electronic transaction communication records) to include all of the following kinds of information<sup>3</sup>:

1. All phone numbers, email addresses, and screen names associated with an individual;
2. The individual associated with any phone number, email address, or screen name;
3. All mailing address, phone number, and billing information associated with an individual and the length of time an individual has subscribed to a service;

---

<sup>2</sup> The President's Review Group on Intelligence and Communications Technologies, *Final Report* 90 (2013).

<sup>3</sup> See Daniel Koffsky, *Requests for Information Under the Electronic Communications Privacy Act*, in *32 Opinions of the Office of Legal Counsel* 2, 5 (2008); President's Review Group, *supra* note 2, at 90; Chris Soghoian, *US Surveillance Law May Poorly Protect New Text Message Services*, American Civil Liberties Union (Jan. 8, 2013, 9:44 AM), <https://www.aclu.org/blog/national-security-technology-and-liberty/us-surveillance-law-may-poorly-protect-new-text>; *National Security Letters*, Electronic Privacy Information Center (last visited Mar. 13, 2014, 4:35 PM), <http://epic.org/privacy/ns/>; Decl. in Supp. of Pet. to Set Aside National Security Letter and Nondisclosure Requirement In re Matter of National Security Letters 5, 11, Mar. 14, 2013, ECF 13-1165; Declaration of Under Seal in Support of Petition to Set Aside National Security Letters and Nondisclosure Requirements Imposed in Connection Therewith, In re Matter of National Security Letters, No. CV-131165 (LB) (N.D. Cal. Mar. 14, 2013), Exhibit A.

4. All IP addresses from which a user has logged into an email account and the timeframes during which each was used;
5. A complete list of all phone calls ever associated with a phone number including, for each call, whether it was outgoing or incoming, the phone number contacted, how long the call lasted, and when it was made;
6. A complete list of all text messages ever associated with a phone number including, for each message, whether it was sent or received, the phone number contacted, and when it was sent; and
7. A complete list of all emails ever associated with a screen name, including, for each email, whether it was sent or received, the email address contacted, other email addresses that were copied, the size of the message, and when it was sent.

These NSL-obtained data, colloquially referred to as “metadata,” generally are considered “non-content” under the definition of “contents” in 18 U.S.C. § 2510(8).<sup>4</sup> But the data demanded by NSLs, while legally non-content data, are in fact profoundly meaningful. As discussed further in section II, information from NSLs can expose details ranging from political beliefs and affiliations to the structure of grassroots organizations to reproductive choices to medical conditions

---

<sup>4</sup> See Decl. Set Aside 9, 15, ECF 13-1165.

and more. As former Google Senior Privacy Analyst and privacy/surveillance author Susan Landau stated in an interview: “The public doesn’t understand . . . It’s much more intrusive than content.” The government gains expansive private information by studying “who you call, and who they call. If you can track that, you know exactly what is happening—you don’t need the content.”<sup>5</sup>

The ECPA NSL substantive provisions authorize the FBI to demand not only many kinds of substantive data, but also data relating to nearly any American. In contrast to older versions of the statute, the current “very low” relevance standard authorizes the FBI to demand data on individuals who are not investigation targets and eliminates any requirement to record particularized facts justifying why an individual’s data are relevant.<sup>6</sup> The only limits on what can be deemed “relevant” are that investigations to which data are relevant must be authorized and that the FBI must be able to justify—almost always to itself rather than a court—that the request is motivated by more than a First Amendment-protected activity alone. § 2709(b). The administration has recently argued that “‘relevance’ is a broad standard that permits discovery of large volumes of data in

---

<sup>5</sup> Jane Mayer, *What’s the Matter With Metadata?*, New Yorker (June 6, 2013), <http://www.newyorker.com/online/blogs/newsdesk/2013/06/verizon-nsa-metadata-surveillance-problem.html> (quoting interview with Landau) (internal quotation marks omitted).

<sup>6</sup> President’s Review Group, *supra* note 2, at 90.

circumstances where doing so is necessary to identify much smaller amounts of information within that data that directly bears on the matter being investigated.”<sup>7</sup>

The substantial lack of affirmative judicial approval in determining what is sufficiently relevant contrasts starkly with other provisions of ECPA and Section 215 of the Patriot Act, statutes governing the collection of similar data but requiring a court order or subpoena. 18 U.S.C. § 2703(c)(1); 50 U.S.C. § 1861. This contrast drove the President’s Review Group on Intelligence and Communications Technologies to observe that it was “unable to identify a principled reason why NSLs should be issued by FBI officials” rather than by a court.<sup>8</sup>

In practice, the expansive relevance standard has facilitated the use of NSLs in “approximately one-third of all counterterrorism, counterintelligence, and cyber investigations” during 2006.<sup>9</sup> When the FBI issues these NSLs, they include one or more requests for either “toll billing records” (telephony and text-message data), “electronic communications transactional records” (email data), or subscriber

---

<sup>7</sup> *Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act 2* (Aug. 9, 2013).

<sup>8</sup> President’s Review Group, *supra* note 2, at 93.

<sup>9</sup> U.S. Department of Justice Office of the Inspector General, *A Review of the FBI’s Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* 109 (2008).

information (names and other identifying data associated with an account). A response to any individual request will thus include hundreds to hundreds of thousands of individual observations—including, for example, a 26-minute call from a subscriber to a phone number the FBI has identified as belonging to his mother, at 10:35 PM six months ago.

As shown in Table I, even the limited unclassified information available indicates that the FBI has made over 300,000 NSL requests in the past decade, the “overwhelming majority” of which have been for ECPA NSL data.<sup>10</sup> Of these, the FBI has made almost 150,000 requests for non-subscriber information of U.S. persons, mostly toll billing or electronic transaction records, and over 165,000 requests (with estimates above 340,000)<sup>11</sup> for information about U.S. persons, including subscriber information. Including requests for information about non-

---

<sup>10</sup> U.S. Department of Justice Office of the Inspector General, *A Review of the FBI’s Use of National Security Letters* 36 (2007); accord OIG (2008), *supra* note 9, at 60, 107; President’s Review Group, *supra* note 2, at 90.

<sup>11</sup> The only public information about requests for subscriber-only information about U.S. persons are that such requests made up 56% of total requests for U.S. persons’ information in 2006, Table I, and the majority of requests in 2012, President’s Review Group, *supra* note 2, at 90. If subscriber-only requests for data about U.S. persons comprised 56% of all requests for data about U.S. persons in all years, as it did in 2006, then the FBI would have made 342,868 total requests for U.S. persons’ data.

Americans, the FBI made over 304,000 requests (with estimates above 570,000).<sup>12</sup> Collectively, these requests have generated databases with millions of observations of phone calls, emails, and text messages.<sup>13</sup>

---

<sup>12</sup> To estimate total requests for persons of any nationality in years other than 2006, we assume that the proportion of total requests that were requests for U.S. persons' data in these years equaled that in 2006, 60%, OIG (2008), *supra* note 9, at 108. Combined with the data for 2006, this yields an estimate of 571,446 total requests.

<sup>13</sup> Though the precise size of the database is not public, it is possible to estimate. Table I shows that the FBI made 149,663 total requests for non-subscriber information pertaining to U.S. citizens. If the FBI made 228,579 requests for information about non-U.S. persons, *see* notes 2-3, *supra* (estimating 571,446 total requests of which 342,868 pertained to U.S. citizens), and 44% of these were for toll billing records or electronic transaction communications records, *see* Table I row 2006 (showing this proportion for U.S. persons' requests), then it made 99,775 requests for non-subscriber information pertaining to non-U.S. persons, yielding a total database of such information that would include 249,437 requests (149,663 + 99,775). If each request yielded an average of 1,000 observations then the database would have nearly 250 million observations.

TABLE I: NSL REQUESTS FROM 2003 TO 2012, BY REQUEST TYPE				
Year	For U.S. persons' non-subscriber information (mostly toll billing or electronic communications transactional records) <sup>14</sup>	For any U.S. persons' data, including subscriber information <sup>15</sup>	For non-U.S. persons' data of any type <sup>16</sup>	Total requests <sup>17</sup>
2003	6,519	More than 6,519	Classified	39,346
2004	8,943	More than 8,943	Classified	56,507
2005	9,254	More than 9,254	Classified	47,221
2006	12,583	28,827	19,279	49,425
2007	16,804	More than 16,804	Classified	More than 16,804
2008	24,744	More than 24,744	Classified	More than 24,744
2009	14,788	More than 14,788	Classified	More than 14,788
2010	24,287	More than 24,287	Classified	More than 24,287
2011	16,511	More than 16,511	Classified	More than 16,511
2012	15,229	More than 15,229	Classified	More than 15,229
<b>Total known</b>	<b>149,662</b>	<b>More than 165,906</b>	<b>Classified</b>	<b>More than 304,862</b>
<b>Estimated Totals<sup>18</sup></b>	<b>149,662</b>	<b>342,868</b>	<b>99,775</b>	<b>571,446</b>

The full set of individuals whose data the FBI could demand under the relevance standard likely comprises all Americans. Since the FBI uses NSLs to determine a target's "family members, associates, living arrangements, and contacts," an authorized agent may deem data pertaining to individuals far

<sup>14</sup> Data in this column for from 2003-2005 from 2007 OIG Report, *supra* note 9, at xx. Data for 2006-2012 from annual reports the FBI has made to Congress, *available at* <https://www.fas.org/irp/agency/doj/fisa/#rept>. Note that these data may include some additional requests for other types of NSL information authorized by statutes other than ECPA (see 2007 OIG Report at xx).

<sup>15</sup> Data in this column from 2008 OIG Report, *supra* note 9, at 108.

<sup>16</sup> Data in this column from 2008 OIG Report, *supra* note 9, at 108.

<sup>17</sup> Data in this column derived from OIG 2007 Report, *supra* note 9, at xvi, xix; OIG 2008 Report at 110. These figures include requests that the FBI failed to report to Congress but that the OIG found in its review of the FBI-OGC NSL database as of May 2006, May 2007.

<sup>18</sup> *See* notes 2-4, *supra*.

removed from an investigation target to be “relevant.”<sup>19</sup> A 2010 OIG investigation found that the FBI has regarded the personal data of any individual within an investigation target’s “community of interest” or “calling circle” to be relevant, though the definitions of these terms were redacted.<sup>20</sup> Revealingly, the 2007 OIG investigation could not find FBI guidance discouraging case agents from using NSLs to access the data of individuals “two or three steps removed” from an investigation target.<sup>21</sup> This is the same standard used by the NSA and means, for example, that if investigation target Adam called Betsy (step one), who emailed Caleb (step two), who texted Dwayne (step three), then Dwayne’s data would be deemed “relevant” to the investigation of Adam.

Though three steps may seem trivial, some estimate that “[i]f the average person called 40 unique people, a three hop [or step] analysis would allow the government to mine the records of 2.5 million Americans when investigating one suspected terrorist.”<sup>22</sup> Others have estimated that the FBI could deem “the phone

---

<sup>19</sup> OIG (2007), *supra* note 10, at xxiv.

<sup>20</sup> U.S. Department of Justice Office of the Inspector General, *A Review of the Federal Bureau of Investigation’s Use of Exigent Letters and Other Informal Requests for Telephone Records* 75 (2010).

<sup>21</sup> OIG (2007), *supra* note 10, at 109.

<sup>22</sup> Pete Yost & Matt Apuzzo, *With 3 ‘Hops,’ NSA Gets Millions of Phone Records*, Associated Press (Jul. 31, 2013 6:19 PM), <http://bigstory.ap.org/article/senate-panel-looking-limits-surveillance>.



records of a sizable proportion of the United States population” to be relevant to a single terrorism investigation under a three-steps rule.<sup>23</sup> Moreover, both of these estimates consider only steps among phone calls; the addition of texts and emails expands the circle of relevant individuals and businesses exponentially. Thus, with millions of Americans’ data considered relevant to any investigation and thousands of investigations each year, a three-steps definition of relevance is a largely empty check on FBI discretion.

According to the 2007 OIG report, once the FBI receives data responding to an NSL request, that data is typically uploaded to a number of different databases. Electronic communications transactional records are uploaded to the Automated Case Support System, the FBI’s centralized case management system. Roughly 34,000 individuals had access to this system in 2005. Toll billing records are uploaded to the Telephone Applications database. Some 19,000 individuals had access to this database in 2006.<sup>24</sup> In addition, information from NSL demands is stored separately in a number of classified databases about which no information

---

<sup>23</sup> Jonathan Mayer & Patrick Mutchler, *MetaPhone: The NSA Three-Hop, Web Policy* (Dec. 9, 2013), <http://webpolicy.org/2013/12/09/metaphone-the-nsa-three-hop/>.

<sup>24</sup> OIG (2007), *supra* note 10, at 28-30.

has been made public.<sup>25</sup> Supplementing these storage databases, the FBI also uses a data analysis application called the Investigative Data Warehouse, which can pull data from each of these databases and run analytic models to reveal data patterns that may be of interest to investigators.<sup>26</sup>

Thousands of non-FBI personnel also have direct access to these databases.<sup>27</sup> Others are often recipients of FBI-produced intelligence products, which are regularly derived from NSL-data analysis and provided to entities including the CIA, NSA, DIA, Joint Terrorism Task Forces at the federal, state, and local levels, foreign governments, U.S. Attorneys' offices, and the FISA Court.<sup>28</sup>

Given the vast authority the ECPA NSL provisions grant to the FBI to collect and store these massive amounts of data, it is unsurprising that reports have surfaced documenting the FBI's abuse of its NSL authority. Due to the low relevance standard, the FBI has relied upon the NSL process to conduct fishing

---

<sup>25</sup> *Id.*

<sup>26</sup> *Id.*

<sup>27</sup> *Id.*

<sup>28</sup> *Id.* at xxiii.

expeditions before it can support a subpoena or FISA court order.<sup>29</sup> In at least one instance, moreover, a FISA court twice *denied* the FBI access to data under Section 215, citing First Amendment concerns. In response to this denial, the FBI issued NSLs based on an identical factual predicate to the Section 215 order, gathering the same data outside the eyes of the FISA court, even though “NSLs have the same First Amendment caveat as Section 215.”<sup>30</sup>

In others cases, NSL recipients have given the FBI information that exceeded the scope of the NSL, pertained to the wrong individuals, or covered the wrong time period, and the FBI failed to destroy the irrelevant data.<sup>31</sup> NSLs have been signed by individuals who were not authorized agents<sup>32</sup> and have been issued in connection with unauthorized investigations,<sup>33</sup> both in violation of the terms of 18 U.S.C. § 2709. Moreover, though a Presidential Order requires the FBI to report all such intelligence violations to the President’s Intelligence Oversight Board, the FBI failed to report one or more violations in 22% of the cases in the OIG’s

---

<sup>29</sup> See U.S. Department of Justice Office of the Inspector General (OIG), *A Review of the Federal Bureau of Investigation’s Use of National Security Letters* xxiv (2007).

<sup>30</sup> U.S. Department of Justice Office of the Inspector General, *A Review of the FBI’s Use of Section 215 Orders for Business Records in 2006* 5 (2008).

<sup>31</sup> OIG (2008), *supra* note 9, at 100.

<sup>32</sup> OIG (2010), *supra* note 20, at 75.

<sup>33</sup> OIG (2007), *supra* note 10, at 66-67.

sample.<sup>34</sup> Furthermore, between 2003-2005, the FBI also failed to report almost 4,600 NSLs to Congress—nearly all ECPA NSLs—as required by § 2709.<sup>35</sup>

Separate from but related to the NSL process, the FBI for many years issued so-called exigent letters, demanding the kinds of data available through NSLs but circumventing even the procedures for issuing NSLs. These letters were often structured to include a promise from the FBI of “legal process to follow,” such as a subpoena or NSL.<sup>36</sup> In one instance, the FBI used an exigent letter to gather reporter and news organization telephone data following a media leak constituting protected First Amendment speech.<sup>37</sup> It entered these records into its NSL databases, where they remained for three years until discovered by the OIG.<sup>38</sup>

## II. NSL DATA REVEAL DEEPLY SENSITIVE INFORMATION ABOUT INDIVIDUALS AND THEIR ASSOCIATIONS

The types of data that can be obtained by NLSs reveal a wide variety sensitive information about the individuals from which the information comes and their associations, beliefs, speech and activities. Despite government claims that the collected data is “just metadata” and do “not include any information about the

---

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*

<sup>36</sup> OIG (2010), *supra* note 20, at 65.

<sup>37</sup> *Id.* at 89-122.

<sup>38</sup> *Id.* at 278.

content” of phone calls, text messages, and emails, NSL data often can reveal information of the same character as that which could be obtained by listening in on a phone call or reading a text or email.<sup>39</sup>

In many instances, “non-content” data, such as NSL data, may be of even more value to government officials than content data. Since substantial non-content data analysis can be automated, non-content data surveillance often yields substantive information cheaper and faster than approaches such as traditional wiretapping, which can be more labor intensive.<sup>40</sup> And unlike content data, the routine creation of non-content is often unavoidable and unprotectable. As computer scientist Matt Blaze noted, “we leave trails of metadata [non-content data] everywhere, anytime we reach out to another person.” There is almost no existing way to dust these trails.<sup>41</sup> Due to § 2709’s broad scope, the relatively low cost of analysis, and the unprotected nature of non-content data, the FBI can use NSLs to determine everything from individuals’ actions, beliefs and religious and political affiliations to organizations’ structures and strategic plans to much more.

---

<sup>39</sup> *Administration White Paper*, *supra* note 7, at 2.

<sup>40</sup> Jane Mayer, *supra* note 5.

<sup>41</sup> See Matt Blaze, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)*, *Wired* (June 16, 2013 9:30 AM), <http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again>.

### **A. Even a Single Call, Text, or E-mail Reveals Sensitive Information**

Though each NSL request can include information on thousands of interactions, a single phone call, text message, or email can already disclose deeply private information.

In many instances, details about the content of a conversation can be deduced from the identity of the parties. Although data that the FBI receives does not explicitly state whom a subscriber has contacted—NSL requests contain telephone numbers or e-mail addresses, not names—it is trivially easy for the FBI to match these data to specific individuals. One way to do so is to issue another NSL. An even more straightforward approach is to conduct a search for a number or address either online or through a public database. Consider, for example, the phone number 916.446.5247, which a Google search can instantly connect to Planned Parenthood Affiliates of California. Or the email pacificregion@aa.org, which, even without a Google search, one could associate with Alcoholics Anonymous. More generally, research shows that the government can link identities associated with lesser-known phone numbers just as easily.<sup>42</sup>

---

<sup>42</sup> See Rebecca J. Rosen, *Stanford Researchers: It is Trivially Easy to Match Metadata to Real People*, The Atlantic (Dec. 24, 2013 1:50 PM), <http://www.theatlantic.com/technology/archive/2013/12/stanford-researchers-it-is-trivially-easy-to-match-metadata-to-real-people/282642>; Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, Web Policy (Mar. (continued on next page)

With just the identity of the other side of a record, the FBI can already learn sensitive information about an individual. For example, certain phone lines are reserved for a specific purpose: support hotlines for rape victims, domestic violence victims, people contemplating suicide, or “listening lines” for gay and lesbian youths.<sup>43</sup> Such hotlines exist for veterans, first responders, drug addicts, gambling addicts, and child abuse victims.<sup>44</sup> Similarly, almost every federal, state, and local agency, including the FBI, has established hotlines for reporting fraud and misconduct by both internal and external sources.<sup>45</sup> Likewise, some email addresses are allocated to particular objectives, such as tipping off reporters about a potential story.<sup>46</sup> A 30-minute call or a lengthy email to any of these hotlines

---

(footnote continued from previous page)

12, 2014), <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata> (finding that simple Google searches and a cheap, consumer-oriented data tool could match 91% of a random sample of 100 phone numbers to specific individuals).

<sup>43</sup> See, e.g., *Gay, Lesbian, Bisexual and Transgender National Hotline*, GLBT National Help Center (last visited Mar. 11, 2014), <http://www.glbtnationalhelpcenter.org/hotline>.

<sup>44</sup> See, e.g., *Childhelp National Child Abuse Hotline*, Childhelp (last visited Mar. 14, 2014), <http://childhelp.org/pages/hotline-home>.

<sup>45</sup> See, e.g., Barton Gellman, *NSA Statements to the Post*, Wash. Post, Aug 15, 2013, <http://wapo.st/1ixchnm>; *Reporting Income Tax Fraud*, State of California Franchise Tax Board (last visited Mar. 17, 2014), [https://www.ftb.ca.gov/online/Fraud\\_Referral/important\\_information.asp](https://www.ftb.ca.gov/online/Fraud_Referral/important_information.asp).

<sup>46</sup> See New York Times, *Contact the Public Editor*, NYTimes.com (last visited Mar. 18, 2014), <http://publiceditor.blogs.nytimes.com/contact-the-public->  
(continued on next page)

reveals information that anyone would consider private. In each of these cases, even without knowing a single word of the phone conversation or email exchange, NSL data from the interaction discloses meaningful clues as to the underlying content. Though these hotlines and tip lines are meant to allow vital, anonymous expression, NSLs allow the FBI to strip away that safety and anonymity and expose both the individual and effectively the content of his or her speech.

In an empirical study highlighting the significance of NSL data in these situations, Stanford University researchers Jonathan Mayer and Patrick Mutchler demonstrated that substantial personal information could be revealed through a single phone call. Analyzing data from 546 volunteers' phone calls to 33,688 unique numbers, Mayer and Mutchler discovered that a large proportion of participants contacted "sensitive organizations" in their daily lives.<sup>47</sup> The table below shows the proportion of volunteers who made at least one call to an organization whose purpose revealed sensitive information about the caller:

---

(footnote continued from previous page)

editor/; Mail & Guardian, *Story Tip-Offs* (last visited Mar. 18, 2014), <http://mg.co.za/page/story-tip-offs>.

<sup>47</sup> Mayer & Mutchler, *supra* note 42 ("phone metadata is unambiguously sensitive, even in a small population and over a short time window. We were able to infer medical conditions, firearm ownership, and more, using solely phone metadata.").



Category	Participants with $\geq 1$ Calls
Health Services	57%
Financial Services	40%
Pharmacies	30%
Veterinary Services	18%
Legal Services	10%
Recruiting and Job Placement	10%
Religious Organizations	8%
Firearm Sales and Repair	7%
Political Officeholders and Campaigns	4%
Adult Establishments	2%
Marijuana Dispensaries	0.4%

As several of these categories suggest, NSL data from a single interaction can reveal sensitive information about possible civil legal disputes or criminal activity. Sensitive information obtained through NSLs is shared with U.S. Attorney's Offices,<sup>48</sup> and a call to a marijuana dispensary, an email to CustomerService@GunsAmerica.com, or a text message to a known gang member, could all serve as reason to begin an investigation or as evidence in a later criminal case, even where the individual was not suspected of anything at the time of the NSL. Contacting a defense attorney may even indicate concerns about criminal activity.

Furthermore, how and when governmental authorities act on these potentially incriminating communications depends solely on their interpretation of

---

<sup>48</sup> OIG (2007), *supra* note 10, at xxiii.

the data. If the picture that NSL data paints is inaccurate or incomplete, it can lead to unnecessary arrests, unexplained detentions, or at the very least, a further invasion of an individual's privacy through additional searches.<sup>49</sup>

In the extreme, NSL data can reveal information even more sensitive than the actual contents of the communication itself. Consider, for instance, the case of text message donation hotlines. Set up as partnerships between wireless telephone carriers and non-profit organizations, these donation hotlines enable wireless subscribers to donate to charities through cellular text messages. By sending a message to a predetermined phone number, a subscriber triggers the wireless carrier to make a donation and add the amount to his monthly bill. In one such program to support of victims of the Haitian earthquake, the American Red Cross enabled thousands of subscribers to text HAITI to 90999 to donate \$10.<sup>50</sup>

In recent years, text-message donation hotlines have gained popularity and expanded to numerous organizations such as churches, cancer research

---

<sup>49</sup> See Griffin Boyce and Brian Duggan, *The Real Reason Why Metadata Collecting Is Dangerous*, New America Foundation (June 17, 2013 4:54 PM), <http://inthewalk.newamerica.net/blog/2013/06/real-reason-why-metadata-collecting-dangerous>.

<sup>50</sup> See Declaration of Edward W. Felten, *ACLU v. Clapper*, No. 13-cv-03994 (WHP) (S.D.N.Y. Aug. 23, 2013), ECF No. 27 (“Felten Decl.”), 16.

foundations, and reproductive services organizations like Planned Parenthood.<sup>51</sup> After a policy change by the Federal Election Commission in 2012, these programs have even invaded electoral campaigns. Candidates such as Barack Obama and Mitt Romney raised money directly via text messages.<sup>52</sup>

In these interactions, the significant information—the identity of the recipient organization and size of the donation—is contained in the NSL data, not in the content of text messages such as “HAITI.” The NSL data alone is sufficient to determine whether the sender was donating (and how much) to a church, Planned Parenthood, or a particular political campaign.

#### **B. Patterns of Calls, Texts, and Emails Reveal Even More Sensitive Information**

In addition to inferences from a single communication, the FBI can gain a far richer and more deeply revealing picture of the contours of a person’s life using data-analysis techniques that assess patterns of activity—who an individual contacts, how frequently, and when. By analyzing the hundreds to hundreds of thousands of data points returned in response to each NSL request, the FBI can

---

<sup>51</sup> See *Donate by Text*, Susan G. Komen for the Cure (last visited Mar. 11, 2014), <http://ww5.komen.org>.

<sup>52</sup> See, e.g., Dan Eggen, *Text ‘Give’ to Obama: President’s Campaign Launches Cellphone Donation Drive*, Wash. Post (Aug. 23, 2012), [http://www.washingtonpost.com/politics/text-give-to-obama-presidents-campaign-launches-cellphone-donation-drive/2012/08/23/5459649a-ecc4-11e1-9ddc-340d5efb1e9c\\_story.html](http://www.washingtonpost.com/politics/text-give-to-obama-presidents-campaign-launches-cellphone-donation-drive/2012/08/23/5459649a-ecc4-11e1-9ddc-340d5efb1e9c_story.html).

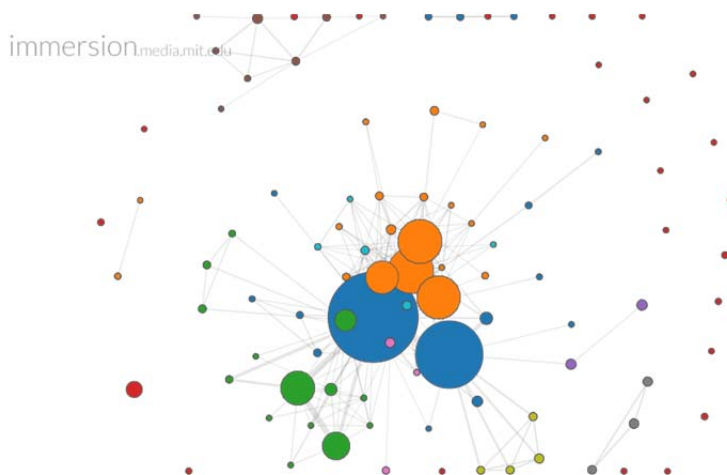
learn an individual's religion, sleep patterns, work habits, hobbies, number and location of friends, and even civil and political affiliations. By combining data from multiple requests about multiple individuals, the FBI can deduce the nature and function of entire organizations, and how the people within them interact.

### **1. Social Graph and Predictive Modeling Techniques are Easy to Implement and Immensely Informative**

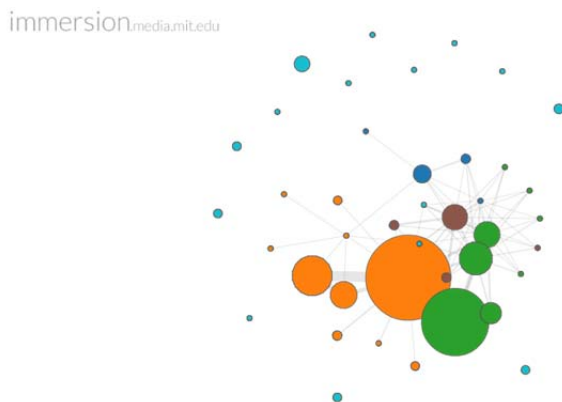
The recent evolution of two tools, social graphs and predictive modeling, add particular potency to the aggregation of data gathered through NSLs. With respect to the first, publicly available software packages can generate social graphs from datasets such as the FBI's NSL database. These software packages take a dataset of non-content data and output a graphical image of an individual's patterns of communication or of communications among members of a group. Consider two such software packages: MIT's Immersion and IBM's i2 Analyst's Notebook.

MIT's Immersion uses the "From, To, Cc and Timestamp" fields of a person's emails—all included in response to NSL requests for electronic transaction communications records—to create a "people-centric view" of that person's life. In under a minute, the software churns through thousands of emails and spits out a network of individuals and organizations with which the user has communicated, highlighting key contacts and linking contacts with each other. By tracking interactions across time, Immersion can also trace the development of relationships. Based on the frequency of the emails exchanged, the software

visualizes a growth or contraction of connections between not only the original user, but also other individuals in his network, detailing his “personal and professional history.”<sup>53</sup>



**Figure 1: An Immersion user's network, visualized as a social graph**



**Figure 2: The Immersion user's network a week earlier. The expansion and contraction of circles provide a visual interpretation of relationship development between individuals in the network.**

---

<sup>53</sup> See *Immersion*, MIT Media Lab (last visited Mar. 17, 2014), <https://immersion.media.mit.edu>.

IBM's more sophisticated i2 Analyst's Notebook software uses the same basic ideas to identify key people, events, and connections in networks described by much larger datasets.<sup>54</sup> For example, the Environmental Investigation Agency used Analyst's Notebook to process non-content data from undercover investigations in order to accurately map out a criminal international tiger trafficking network.<sup>55</sup>

Either in conjunction with or independent of social graphs, the FBI can also use predictive modeling to derive sensitive information about individuals and groups from the data it has gathered through NSLs. Predictive models allow analysts to use known patterns of activity to make specific and highly accurate predictions about individual and organizational attributes, such as race, religion, or leadership structure. For example, happily married couples often call each other many times a week. If an analyst applied a predictive model based on this pattern to a set of toll billing records for an individual who had called her spouse infrequently for many months, the model might indicate that she had between a predictable chance of filing for divorce within one year.

---

<sup>54</sup> See *Analyst's Notebook*, IBM (last visited Mar. 17, 2014), <http://www-03.ibm.com/software/products/en/analysts-notebook-family>.

<sup>55</sup> See IBM, *Environmental Investigation Agency: IBM i2 Solution Help Combat the Illegal Tiger Trade* (2012).

The larger the dataset a researcher has upon which to build a predictive model, the more precise the model will be. If a certain calling pattern is only seen in a few married couples, then applying a model based on that pattern to new data will yield only weak inferences. But if the same pattern is seen in 5,000 couples, a model based on the pattern will offer opportunities to ask nuanced queries and make inferences with confidence. For instance, a researcher could query the likelihood of divorce in six months and in two years, and the confidence intervals around results might be plus or minus 5% rather than 10%. Given the vast data set that NSLs provide—including hundreds of millions of observations, as estimated above—it is almost certain that FBI researchers have created sophisticated and highly precise predictive models. Even if they have not, there is an extensive public literature on predictive modeling upon which the Bureau can draw.

Though the FBI has developed its data-analysis tools in order to improve its terrorism and espionage investigations, these dual-use tools are even easier to apply to ordinary Americans. As Matt Blaze argues, “[t]he better understood the patterns of a particular group’s behavior, the more useful it is. This makes using metadata [non-content data] to identify lone-wolf Al Qaeda sympathizers (a tiny minority about whose social behavior relatively little is known) a lot harder than, say, rooting out Tea Partiers or Wall Street Occupiers, let alone the people with

whom we share our beds.”<sup>56</sup>

## 2. NSL Data Reveal Extensive Private Personal, Political, Associational, Religious, Corporate, Medical, and Financial Information

As we lack access to the FBI’s massive database of NSL data, we cannot say with precision what applying social graphs and predictive models to this data would reveal. But even relatively naïve analyses of this data yields information on medical conditions, religious affiliations, relational and political networks, corporate structures, and finances. Comprehensively applying social graphs and predictive modeling to millions of observations would only increase the sensitivity of many of these inferences.

First, information obtained through NSLs can reveal substantial information about the operations of political groups. A social graph derived from NSL data can reveal an association’s otherwise anonymous membership, donors, political supporters, and confidential sources. As former NSA official William Binney has stated, the government could use data analysis to “monitor the Tea Party, or reporters, whatever group or organization you want to target. . . It’s exactly what

---

<sup>56</sup> Matt Blaze, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)*, Wired (June 16, 2013 9:30 AM), <http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again>.



the Founding Fathers never wanted.”<sup>57</sup> Even a cursory analysis of the frequency of communications among members could distinguish who within a grassroots movement is an ardent organizer and who is a casual participant. With more detailed study, as Susan Landau noted, non-content data can even show “if opposition leaders are meeting, who is involved, where they gather, and for how long.”<sup>58</sup>

Second, NSL data disclose a great deal about the strength of personal relationships. Generally, a person one calls once a week is more likely to be a close friend than someone one calls once a year.<sup>59</sup> More specifically, consider an NSL request made with regards to a man in an illicit intimate relationship. The data returned in reply to this request might show he makes long, frequent calls to his mistress late at night, in contrast to the short, sparse calls made to his wife. Eventually, the affair may end, and the frequency of the calls to the mistress might drop or end entirely. Or, perhaps the affair continues and he begins to communicate frequently with an attorney specializing in divorce. Precisely in this vein, it was FBI analysis of non-content data similar to NSL data that ultimately

---

<sup>57</sup> Jane Mayer, *supra* note 5 (quoting interview with Binney) (internal quotation marks omitted).

<sup>58</sup> Jane Mayer, *supra* note 5 (quoting interview with Susan Landau).

<sup>59</sup> *See* Felten Decl., 17.

revealed former CIA director David Petraeus's affair with Paula Broadwell. While looking into allegations of another sort, the FBI linked together multiple email addresses used by Broadwell to uncover the affair that ended both participants' public careers.<sup>60</sup>

Third, the FBI can easily infer religious affiliation and association from information gained through NSLs. On the most basic level, adherents of particular religions likely call organizations affiliated with their religion more often than they call organizations affiliated with other religions. Relying only on "the naïve assumption" that this is true, Mayer and Mutchler accurately identified the religion of 73% of participants.<sup>61</sup>

Additionally, adherents of different religions may exhibit notable patterns of phone calls, emails, and text messages. For example, the NSL data of an individual who strictly observes the Sabbath would show no communications on Saturdays, while that of an individual who regularly attends church on Sunday mornings would show little activity at that time. NSL data of an individual who is Muslim

---

<sup>60</sup> See Hal Hodson, *How Metadata Brought Down CIA Boss David Petraeus*, NewsScientist (Nov. 16, 2013 1:59 PM), <http://www.newscientist.com/article/dn22511-how-metadata-brought-down-cia-boss-david-petraeus.html>.

<sup>61</sup> Mayer & Mutchler, *supra* note 42.

and recites the Isha prayer nightly might show more activity between dawn and dusk if that individual communicates with others before or after prayers.

Furthermore, on an organizational level, a social graph of email data could disclose a network of friends who frequent the same religious services. An evolution of this social graph over time could reveal when an individual changed faiths or began to frequent a different place of worship. It could also show who manages the religious social community, which members are most active, and to whom certain members turn for advice at critical moments.

Fourth, NSL data can reveal internal or external dynamics within the corporate sector. For example, NSL data can reveal the relative power of employees within a firm. As *The Economist* observed: “People at the top of the office or social pecking order often receive quick callbacks [and] do not worry about calling other people late at night.”<sup>62</sup> The lengths of phone calls can also be indicative: “Influential [people] reveal their clout by making long calls, while the calls they receive are generally short.”<sup>63</sup>

NSL data can also expose valuable information about a company’s future. Multiple calls among a subset of the members of a board of directors over a short

---

<sup>62</sup> *Mining Social Networks: Untangling the Social Web*, *Economist* (Sept. 2, 2010), <http://www.economist.com/node/16910031>.

<sup>63</sup> *Id.*

period of time and soon before a board meeting might evince intentions to stage a corporate takeover. Correspondence by executives at a smaller firm with those at a larger competing firm, and then investment banks and attorneys who specialize in acquisitions, could indicate a coming sale of the company.

Fifth, NSL data can reveal substantial information about someone's personal finances. As noted above, Mayer and Mutchler found that over half of individuals in their sample called at least one of their financial institutions over only the few-month time horizon of their study. An individual in debt would have frequent contact with entities identifiable as debt collectors and might contact payday loan services or an attorney who specializes in Chapter 7 bankruptcy filings. Someone who provides funds to a relative abroad might receive more emails from Western Union than is typical and might contact foreign banking organizations. Moreover, NSL data obtained through ECPA's provisions is only one subset of all NSL data that the FBI can collect. Other statutes provide authority to demand full credit reports, for example, data that could quickly corroborate evidence derived from ECPA NSLs.

Finally, patterns in data obtained through FBI use of NSLs can reveal an enormous amount of sensitive information about medical conditions. Consider, for instance, the inferences derived from personal records showing "a call to a gynecologist, and then a call to an oncologist, and then a call to close family

members.”<sup>64</sup> Mayer and Mutchler’s study empirically documents this possibility. Relying on patterns of phone calls to certain kinds of doctors, laboratories, pharmacies, and home-reporting hotlines, Mayer and Mutchler deduced that one participant in their study suffered from cardiac arrhythmia and another from relapsing multiple sclerosis. For a third, they observed that the participant had a long morning call with her sister, then two days later placed a series of calls to the local Planned Parenthood clinic, placed additional calls to the clinic two weeks later, and then made a final call a month afterwards.<sup>65</sup>

In a different context, a recent, widely reported incident involving Target illustrates how predictive models can enhance these inferences. Using extensive customer data, Target determined that pregnant women are more likely to buy certain products at different stages of pregnancy. To capitalize on this trend, Target used its database to create a “pregnancy prediction” score upon which it based an advertisement campaign offering targeted coupons to women in different trimesters. In so doing, Target discovered incredibly private information about its customers’ reproductive choices and, in at least one case, determined that a teenage girl was pregnant and sent her pregnancy related coupons before even her father

---

<sup>64</sup> Jane Mayer, *supra* note 5 (quoting Susan Landau) (internal quotation marks omitted).

<sup>65</sup> *See* Mayer & Mutchler, *supra* note 42.

found out.<sup>66</sup> These types of patterns that can easily be discerned from aggregated information are often far more revealing than one might ever imagine from any individual piece of data.

## CONCLUSION

The reach of NSL demands for information into the private lives of ordinary Americans is nearly limitless. Contradicting government claims that NSL data does not include content, simple analysis of NSL data can reveal a wide variety of any American's otherwise anonymous political activity or beliefs, close relationships, religious affiliations, personal or community associations, medical records, financial data and more. The FBI can learn deeply sensitive information about the daily life of almost every person in this country without meaningful, affirmative judicial approval.

DATED: March 28, 2014

Respectfully submitted,

JUELSGAARD INTELLECTUAL  
PROPERTY & INNOVATION CLINIC  
Mills Legal Clinic at Stanford Law School

By: /s/ Phillip R. Malone  
Phillip R. Malone  
*Counsel for Amici Curiae*

---

<sup>66</sup> See Charles Duhigg, *How Companies Learn Your Secrets*, NYTimes.com (Feb. 16, 2012), [http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&\\_r=1&hp](http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp).

## STATEMENT OF RELATED CASES

Consolidated cases *Under Seal v. Holder, et al.*, No's. 13-15957 and 13-16731, and *Under Seal v. Holder, et al.*, No. 13-16732, which involve the same legal issues but different NSL recipients, are related. This Court has ordered that No's. 13-15957 and 13-16731 be briefed separately from, but on the same briefing and oral argument schedule as, No. 13-16732.

**CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME  
LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE  
REQUIREMENTS  
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)**

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief *Amici Curiae* complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) and 29(d) because this brief contains 6,925 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word for Mac 2011, the word processing system used to prepare the brief, in 14 point Times New Roman font.

I declare under penalty of perjury that this Certificate of Compliance is true and correct and that this declaration was executed on March 28, 2014.

By: /s/Phillip R. Malone  
Phillip P. Malone

JUELSGAARD INTELLECTUAL  
PROPERTY & INNOVATION CLINIC

*Counsel for Amici Curiae*



# EXHIBIT A

## EXHIBIT A

### List of *Amici* and Short Biographies<sup>1</sup>

**Harold Abelson** is a Professor in the Department of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology. A fellow at the Institute of Electrical and Electronic Engineers (IEEE), he was awarded the 2011 Association for Computing Machinery (ACM) Special Interest Group on Computer Science Education Award for Outstanding Contribution to Computer Science Education and the 2012 ACM Karl V. Karlstrom Outstanding Educator Award. Professor Abelson's research interests focus on information technology and policy; he is also an advocate of intellectual property reform, innovation, and an open Internet. His publications include *Access Control is an Inadequate Framework for Privacy Protection* and *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion*.

**Andrew W. Appel** is the Chair of and a Professor in Princeton University's Computer Science Department. He was named an ACM Fellow in 1998 and received the 2002 ACM Special Interest Group on Programming Languages (SIGPLAN) Distinguished Service Award. Professor Appel is active in issues related to the intersection between law and technology, focusing his research

---

<sup>1</sup> Amici file this brief in their individual capacities, not as representatives of the institutions with which they are affiliated.

primarily on program verification, computer security, programming language semantics, and compilers. His publications include Compiling with Continuations and Security Seals on Voting Machines: A Case Study.

**Steven M. Bellovin** is a Professor in the Computer Science Department at Columbia University. He was elected to the National Academy of Engineering in 2001 and awarded the NIST/NSA National Computer Systems Security Award in 2006. Professor Bellovin's research focuses on networks, security, and the tensions between the two. Examples of his publications include Firewalls and Internet Security: Repelling the Wily Hacker, Facebook and privacy: It's complicated, and When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning.

**Matthew A. Blaze** is an Associate Professor in the Computer and Information Science Department at the University of Pennsylvania where he also directs the Distributed Systems Lab Research. He implemented the Cryptographic File System for Unix in 2002, which remains in use today. Professor Blaze's research interests center cryptography and its applications, trust management, human scale security, secure systems design, and networking and distributed computing. Several recent publications include Going Bright: Wiretapping Without Weakening Communication Infrastructure and Notes on Theoretical Limitations and Practical Vulnerabilities of Internet Surveillance Capture.

**Fernando J. Corbato** is Professor Emeritus in the Department of Electrical Engineering and Computer Science at M.I.T. He has achieved wide recognition for his pioneering work on the design and development of multiple-access computer systems. He was associated with the M.I.T. Computation Center from its organization in 1956 until 1966. In 1963 he was a founding member of Project MAC, the antecedent of CSAIL. In 1990, Prof. Corbato received the Turing Award, "for his pioneering work in organizing the concepts and leading the development of the general-purpose, large-scale, time-sharing and resource-sharing computer systems." At his retirement in 1996, Prof. Corbato held a Ford Professor of Engineering Chair.

**Lorrie Faith Cranor** is an Associate Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University. She is also the director of the CyLab Usable Privacy and Security Laboratory. Professor Cranor was the 2006 Phase 1 Winner of the Tor Graphical User Interface Design Competition and 2004 IBM Best Academic Privacy Faculty Award. Her work has been widely recognized, most recently being awarded the Future of Privacy Forum Privacy Papers for Policy Makers 2012 award for Leading Paper. Her research interests focuses on usable privacy and security, with recent publications including The Platform for Privacy Preferences 1.0 (P3P 1.0) Specification and Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences.

**David Farber** is the Distinguished Career Professor of Computer Science and Public Policy in the School of Computer Science at Carnegie Mellon University. He has been a major contributor to the development of computer networking and

computer programming languages. Professor Farber served as Chief Technologist to the FCC from 2000 to 2001 and received the 1995 ACM Special Interest Group on Data Communications Award for lifelong contributions to the computer communications field. His publications include A Secure and Reliable Bootstrap Architecture and Recoverability of Communication Protocols—Implications of a Theoretical Study.

**Edward W. Felten** is is the Robert E. Kahn Professor of Computer Science and Public Affairs, and the Director of the Center for Information Technology Policy, at Princeton University. He has published more than 100 papers in the research literature. In 2011-12 he served as the first Chief Technologist at the Federal Trade Commission. He has testified before Congressional hearings on topic including surveillance and privacy. He is a member of the National Academy of Engineering and the American Academy of Arts and Sciences.

**Michael J. Freedman** is an Associate Professor in the Computer Science Department at Princeton University. His research broadly focuses on distributed systems, security, and networking, and has led to commercial products and deployed systems reaching millions of users daily. His privacy-related research has developed techniques for untrusted and encrypted cloud services, anonymous communication systems, and secure multi-party computation. A recipient of the Presidential Early Career

Award for Scientists and Engineers (PECASE), Freedman has also been recognized by a National Science Foundation CAREER Award, the Office of Naval Research's Young Investigator Award, membership in DARPA's Computer Science Study Group, an Alfred P. Sloan Fellowship, and multiple conference award publications.

**Matthew D. Green** is an Assistant Research Professor in the Department of Computer Science at Johns Hopkins University. He received the 2007 Award for Outstanding Research in Privacy Enhancing Technologies. Professor Green's research interests include privacy-enhanced information storage, anonymous payment systems, and bilinear map-based cryptography as well as cryptographic engineering. His publications include *Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage* and *Security Analysis of a Cryptographically-Enabled RFID Device*.

**J. Alex Halderman** is an Assistant Professor of Electrical Engineering and Computer Science at the University of Michigan. His work has won numerous distinctions, including two best paper awards from the USENIX Security conference. Professor Halderman's research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. His publications include *Telex: Anticensorship in the Network Infrastructure* and *Lest We Remember: Cold-Boot Attacks on Encryption Keys*.

**Robert Harper** is a Professor of Computer Science at Carnegie Mellon University, where he has been a member of the faculty since 1988. His research focuses on the application of constructive type theory, a computationally based foundation for mathematics, to programming languages and program verification. He was elected as an ACM Fellow in July of 2006. He is the co-recipient of the 2006 Most Influential Paper Ten Years Later Award from the ACM Conference on Programming Language Design and Implementation and of the 2007 Test of Time Award from the IEEE Conference on Logic in Computer Science. He is a past editor of the Journal of the ACM, and is currently a member of the editorial board for the Journal of Functional Programming, Information and Computation, and Mathematical Structures in Computer Science. He was honored with the Allen E. Newell Award for Excellence in Research, and the Herbert A. Simon Award for Excellence in Teaching, both at Carnegie Mellon University.

**David Mazieres** is associate professor of Computer Science at Stanford University, where he leads the Secure Computer Systems research group. Prof. Mazieres received a BS in Computer Science from Harvard in 1994 and Ph.D. in Electrical Engineering and Computer Science from MIT in 2000. Prof. Mazieres's research interests include Operating Systems and Distributed Systems, with a particular focus on security. Prof. Mazieres has several awards including a Sloan award (2002), USENIX best paper award (2001), NSF CAREER award (2001),

MIT Sprowls best thesis in computer science award (2000), and fast-track journal papers at OSDI (2000), SOSP (1995), and SOSP (2005).

**Greg Morrisett** is the Allen B. Cutting Professor of Computer Science at Harvard University, where he also served as the Associate Dean for Computer Science and Engineering from 2007-2010. Prof. Morrisett has received a number of awards for his research on programming languages, type systems, and software security, including a Presidential Early Career Award for Scientists and Engineers, an IBM Faculty Fellowship, an NSF Career Award, and an Alfred P. Sloan Fellowship. He was recently made a Fellow of the ACM. He currently serves on the editorial board for The Journal of the ACM and as co-editor-in-chief for the Research Highlights column of Communications of the ACM. In addition, Prof. Morrisett has served on the DARPA Information Science and Technology Study (ISAT) Group, the NSF Computer and Information Science and Engineering (CISE) Advisory Council, Microsoft Research's Technical Advisory Board, and Microsoft's Trustworthy Computing Academic Advisory Board.

**James Purtilo** is an Associate Professor of Computer Science at the University of Maryland, College Park, where he specializes in software producibility and product assurance. Purtilo has published on software formal methods, rapid prototyping and testing, most recently with a focus on mechanisms for intrusion detection and prevention in secure systems. At the University of Maryland, he has



served as director of the Master of Software Engineering Program on his campus, Associate Dean in his college and Chair of CS Department's undergraduate program.

**Ronald L. Rivest** is a Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology. A founder of RSA Security and Peppercoin, Professor Rivest was received the 2012 National Cyber Security Hall of Fame and 2005 Massachusetts Innovation & Technology Exchange (MITX) Lifetime Achievement Award. His research primarily focuses on cryptography and computer and network security. His recent publications include *Introduction to Algorithms* and *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*.

**Avi Rubin** is a Professor of Computer Science at Johns Hopkins University and Technical Director of the Johns Hopkins Information Security Institute. He was the Director of the USENIX Association from 2000 to 2004 and a recipient of the 2007 Award for Outstanding Research in Privacy Enhancing Technologies. His research primarily focuses on computer security. His recent publications include *Charm: A Framework for Rapidly Prototyping Cryptosystems* and *Security and Privacy in Implantable Medical Devices and Body Area Networks*.

**Barbara Simons** is retired from IBM Research. She is the only woman to have received the Distinguished Engineering Alumni Award from the College of

Engineering of U.C. Berkeley. A fellow of the American Association for the Advancement of Science (AAAS) and a fellow and former president of the Association for Computing Machinery (ACM), she has also received the Computing Research Association Distinguished Service Award. An expert on electronic voting, Simons recently published *Broken Ballots: Will Your Vote Count?*, a book on voting machines co-authored with Douglas Jones. She was appointed to the Board of Advisors of the U.S. Election Assistance Commission in 2008, and she was a member of the workshop, convened at the request of President Clinton, that produced a report on Internet Voting in 2001.

**Eugene H. Spafford** is a Professor in the Department of Computer Science at Purdue and serves as the Executive Director of Purdue's Center for Education and Research in Information Assurance and Security. He was an advisor to the National Science Foundation (NSF) and is the Editor-in-Chief of the Elsevier journal, *Computers & Security*. Professor Spafford was inducted into the Cybersecurity Hall of Fame in 2013 and received the 2007 ACM President's Award. His research focuses on preventing, detecting, and remedying information system failures and information security. He has published many articles and books including *Practical UNIX and Internet Security* and *Web Security, Privacy & Commerce*.

**Daniel S. Wallach** is a Professor of Computer Science and a Rice Scholar at the Baker Institute for Public Policy at Rice University. A member of the USENIX Association Board of Directors, he received the 2013 Microsoft Faculty Research Award, 2009 Google Research Award, and 2000 NSF CAREER Award. Professor Wallach's research primarily focuses on computer security and has touched on issues include web browsers and servers, peer-to-peer systems, smartphones, and voting machines. His publications include VoteBox: A Tamper-evident, Verifiable Electronic Voting System and Secure Routing for Structured Peer-to-Peer Overlay Networks.

**CERTIFICATE OF SERVICE**

I certify that I caused the foregoing **BRIEF *AMICI CURIAE* OF EXPERTS IN COMPUTER SCIENCE AND DATA SCIENCE IN SUPPORT OF APPELLANTS** to be delivered to the court by placing the same for Federal Express next-business-day delivery on March 31, 2014, addressed as follows:

Susan Soong, Chief Deputy Clerk - Operations  
U.S. Court of Appeals for the Ninth Circuit  
95 7th Street  
San Francisco, CA 94103

I am informed and believe that the court will effect service on the parties.

Dated: March 31, 2014

/s/ Lynda F. Johnston  
LYNDA F. JOHNSTON

**EXHIBIT S**

[Home](#) • [Briefing Room](#) • [Speeches & Remarks](#)

## The White House

Office of the Press Secretary

For Immediate Release

January 17, 2014

# Remarks by the President on Review of Signals Intelligence

Department of Justice  
Washington, D.C.

11:15 A.M. EST

THE PRESIDENT: At the dawn of our Republic, a small, secret surveillance committee borne out of the “The Sons of Liberty” was established in Boston. And the group’s members included Paul Revere. At night, they would patrol the streets, reporting back any signs that the British were preparing raids against America’s early Patriots.

Throughout American history, intelligence has helped secure our country and our freedoms. In the Civil War, Union balloon reconnaissance tracked the size of Confederate armies by counting the number of campfires. In World War II, code-breakers gave us insights into Japanese war plans, and when Patton marched across Europe, intercepted communications helped save the lives of his troops. After the war, the rise of the Iron Curtain and nuclear weapons only increased the need for sustained intelligence gathering. And so, in the early days of the Cold War, President Truman created the National Security Agency, or NSA, to give us insights into the Soviet bloc, and provide our leaders with information they needed to confront aggression and avert catastrophe.

Throughout this evolution, we benefited from both our Constitution and our traditions of limited government. U.S. intelligence agencies were anchored in a system of checks and balances -- with oversight from elected leaders, and protections for ordinary citizens. Meanwhile, totalitarian states like East Germany offered a cautionary tale of what could happen when vast, unchecked surveillance turned citizens into informers, and persecuted people for what they said in the privacy of their own homes.

In fact, even the United States proved not to be immune to the abuse of surveillance. And in the 1960s, government spied on civil rights leaders and critics of the Vietnam War. And partly in response to these revelations, additional laws were established in the 1970s to ensure that our intelligence capabilities could not be misused against our citizens. In the long, twilight struggle against Communism, we had been reminded that the very liberties that we sought to preserve could not be sacrificed at the altar of national security.

If the fall of the Soviet Union left America without a competing superpower, emerging threats from terrorist groups, and the proliferation of weapons of mass destruction placed new and in some ways more complicated demands on our intelligence agencies. Globalization and the Internet made these threats more acute, as technology erased borders and empowered individuals to project great violence, as well as great good. Moreover, these new threats raised new legal and new policy questions. For while few doubted the legitimacy of spying on hostile states, our framework of laws was not fully adapted to prevent terrorist attacks by individuals acting on their own, or acting in small, ideologically driven groups on behalf of a foreign power.

The horror of September 11th brought all these issues to the fore. Across the political spectrum, Americans recognized that we had to adapt to a world in which a bomb could be built in a basement, and our electric grid could be shut down by operators an ocean away. We were shaken by the signs we had missed leading up to the attacks -- how the hijackers had made phone calls to known extremists and traveled to suspicious places. So we demanded that our intelligence community improve its capabilities, and that law enforcement change practices to focus more on preventing attacks before they happen than prosecuting terrorists after an attack.

It is hard to overstate the transformation America’s intelligence community had to go through after 9/11. Our agencies suddenly needed to do far more than the traditional mission of monitoring hostile powers and gathering information for policymakers. Instead, they were now asked to identify and target plotters in some of the most remote parts of the world, and to anticipate the actions of networks that, by their very nature, cannot be easily penetrated with spies or informants.

And it is a testimony to the hard work and dedication of the men and women of our intelligence community that over the past decade we’ve made enormous strides in fulfilling this mission. Today, new capabilities allow intelligence agencies to track who a terrorist is in contact with, and follow the trail of his travel or his funding. New laws allow

information to be collected and shared more quickly and effectively between federal agencies, and state and local law enforcement. Relationships with foreign intelligence services have expanded, and our capacity to repel cyber-attacks have been strengthened. And taken together, these efforts have prevented multiple attacks and saved innocent lives -- not just here in the United States, but around the globe.

And yet, in our rush to respond to a very real and novel set of threats, the risk of government overreach -- the possibility that we lose some of our core liberties in pursuit of security -- also became more pronounced. We saw, in the immediate aftermath of 9/11, our government engaged in enhanced interrogation techniques that contradicted our values. As a Senator, I was critical of several practices, such as warrantless wiretaps. And all too often new authorities were instituted without adequate public debate.

Through a combination of action by the courts, increased congressional oversight, and adjustments by the previous administration, some of the worst excesses that emerged after 9/11 were curbed by the time I took office. But a variety of factors have continued to complicate America's efforts to both defend our nation and uphold our civil liberties.

First, the same technological advances that allow U.S. intelligence agencies to pinpoint an al Qaeda cell in Yemen or an email between two terrorists in the Sahel also mean that many routine communications around the world are within our reach. And at a time when more and more of our lives are digital, that prospect is disquieting for all of us.

Second, the combination of increased digital information and powerful supercomputers offers intelligence agencies the possibility of sifting through massive amounts of bulk data to identify patterns or pursue leads that may thwart impending threats. It's a powerful tool. But the government collection and storage of such bulk data also creates a potential for abuse.

Third, the legal safeguards that restrict surveillance against U.S. persons without a warrant do not apply to foreign persons overseas. This is not unique to America; few, if any, spy agencies around the world constrain their activities beyond their own borders. And the whole point of intelligence is to obtain information that is not publicly available. But America's capabilities are unique, and the power of new technologies means that there are fewer and fewer technical constraints on what we can do. That places a special obligation on us to ask tough questions about what we should do.

And finally, intelligence agencies cannot function without secrecy, which makes their work less subject to public debate. Yet there is an inevitable bias not only within the intelligence community, but among all of us who are responsible for national security, to collect more information about the world, not less. So in the absence of institutional requirements for regular debate -- and oversight that is public, as well as private or classified -- the danger of government overreach becomes more acute. And this is particularly true when surveillance technology and our reliance on digital information is evolving much faster than our laws.

For all these reasons, I maintained a healthy skepticism toward our surveillance programs after I became President. I ordered that our programs be reviewed by my national security team and our lawyers, and in some cases I ordered changes in how we did business. We increased oversight and auditing, including new structures aimed at compliance. Improved rules were proposed by the government and approved by the Foreign Intelligence Surveillance Court. And we sought to keep Congress continually updated on these activities.

What I did not do is stop these programs wholesale -- not only because I felt that they made us more secure, but also because nothing in that initial review, and nothing that I have learned since, indicated that our intelligence community has sought to violate the law or is cavalier about the civil liberties of their fellow citizens.

To the contrary, in an extraordinarily difficult job -- one in which actions are second-guessed, success is unreported, and failure can be catastrophic -- the men and women of the intelligence community, including the NSA, consistently follow protocols designed to protect the privacy of ordinary people. They're not abusing authorities in order to listen to your private phone calls or read your emails. When mistakes are made -- which is inevitable in any large and complicated human enterprise -- they correct those mistakes. Laboring in obscurity, often unable to discuss their work even with family and friends, the men and women at the NSA know that if another 9/11 or massive cyber-attack occurs, they will be asked, by Congress and the media, why they failed to connect the dots. What sustains those who work at NSA and our other intelligence agencies through all these pressures is the knowledge that their professionalism and dedication play a central role in the defense of our nation.

Now, to say that our intelligence community follows the law, and is staffed by patriots, is not to suggest that I or others in my administration felt complacent about the potential impact of these programs. Those of us who hold office in America have a responsibility to our Constitution, and while I was confident in the integrity of those who lead our intelligence community, it was clear to me in observing our intelligence operations on a regular basis that changes in our technological capabilities were raising new questions about the privacy safeguards currently in place.

Moreover, after an extended review of our use of drones in the fight against terrorist networks, I believed a fresh examination of our surveillance programs was a necessary next step in our effort to get off the open-ended war footing that we've maintained since 9/11. And for these reasons, I indicated in a speech at the National Defense University last May that we needed a more robust public discussion about the balance between security and liberty.

Of course, what I did not know at the time is that within weeks of my speech, an avalanche of unauthorized disclosures would spark controversies at home and abroad that have continued to this day.

And given the fact of an open investigation, I'm not going to dwell on Mr. Snowden's actions or his motivations; I will say that our nation's defense depends in part on the fidelity of those entrusted with our nation's secrets. If any individual who objects to government policy can take it into their own hands to publicly disclose classified information, then we will not be able to keep our people safe, or conduct foreign policy. Moreover, the sensational way in which these disclosures have come out has often shed more heat than light, while revealing methods to our adversaries that could impact our operations in ways that we may not fully understand for years to come.

Regardless of how we got here, though, the task before us now is greater than simply repairing the damage done to our operations or preventing more disclosures from taking place in the future. Instead, we have to make some important decisions about how to protect ourselves and sustain our leadership in the world, while upholding the civil liberties and privacy protections that our ideals and our Constitution require. We need to do so not only because it is right, but because the challenges posed by threats like terrorism and proliferation and cyber-attacks are not going away any time soon. They are going to continue to be a major problem. And for our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world.

This effort will not be completed overnight, and given the pace of technological change, we shouldn't expect this to be the last time America has this debate. But I want the American people to know that the work has begun. Over the last six months, I created an outside Review Group on Intelligence and Communications Technologies to make recommendations for reform. I consulted with the Privacy and Civil Liberties Oversight Board, created by Congress. I've listened to foreign partners, privacy advocates, and industry leaders. My administration has spent countless hours considering how to approach intelligence in this era of diffuse threats and technological revolution. So before outlining specific changes that I've ordered, let me make a few broad observations that have emerged from this process.

First, everyone who has looked at these problems, including skeptics of existing programs, recognizes that we have real enemies and threats, and that intelligence serves a vital role in confronting them. We cannot prevent terrorist attacks or cyber threats without some capability to penetrate digital communications -- whether it's to unravel a terrorist plot; to intercept malware that targets a stock exchange; to make sure air traffic control systems are not compromised; or to ensure that hackers do not empty your bank accounts. We are expected to protect the American people; that requires us to have capabilities in this field.

Moreover, we cannot unilaterally disarm our intelligence agencies. There is a reason why BlackBerrys and iPhones are not allowed in the White House Situation Room. We know that the intelligence services of other countries -- including some who feign surprise over the Snowden disclosures -- are constantly probing our government and private sector networks, and accelerating programs to listen to our conversations, and intercept our emails, and compromise our systems. We know that.

Meanwhile, a number of countries, including some who have loudly criticized the NSA, privately acknowledge that America has special responsibilities as the world's only superpower; that our intelligence capabilities are critical to meeting these responsibilities, and that they themselves have relied on the information we obtain to protect their own people.

Second, just as ardent civil libertarians recognize the need for robust intelligence capabilities, those with responsibilities for our national security readily acknowledge the potential for abuse as intelligence capabilities advance and more and more private information is digitized. After all, the folks at NSA and other intelligence agencies are our neighbors. They're our friends and family. They've got electronic bank and medical records like everybody else. They have kids on Facebook and Instagram, and they know, more than most of us, the vulnerabilities to privacy that exist in a world where transactions are recorded, and emails and text and messages are stored, and even our movements can increasingly be tracked through the GPS on our phones.

Third, there was a recognition by all who participated in these reviews that the challenges to our privacy do not come from government alone. Corporations of all shapes and sizes track what you buy, store and analyze our data, and use it for commercial purposes; that's how those targeted ads pop up on your computer and your smartphone periodically. But all of us understand that the standards for government surveillance must be higher. Given the unique power of the state, it is not enough for leaders to say: Trust us, we won't abuse the data we collect. For history has too many examples when that trust has been breached. Our system of government is built on the premise that our liberty cannot depend on the good intentions of those in power; it depends on the law to constrain those in power.

I make these observations to underscore that the basic values of most Americans when it comes to questions of surveillance and privacy converge a lot more than the crude characterizations that have emerged over the last several months. Those who are troubled by our existing programs are not interested in repeating the tragedy of 9/11, and those who defend these programs are not dismissive of civil liberties.

The challenge is getting the details right, and that is not simple. In fact, during the course of our review, I have often reminded myself I would not be where I am today were it not for the courage of dissidents like Dr. King, who were spied upon by their own government. And as President, a President who looks at intelligence every morning, I



also can't help but be reminded that America must be vigilant in the face of threats.

Fortunately, by focusing on facts and specifics rather than speculation and hypotheticals, this review process has given me -- and hopefully the American people -- some clear direction for change. And today, I can announce a series of concrete and substantial reforms that my administration intends to adopt administratively or will seek to codify with Congress.

First, I have approved a new presidential directive for our signals intelligence activities both at home and abroad. This guidance will strengthen executive branch oversight of our intelligence activities. It will ensure that we take into account our security requirements, but also our alliances; our trade and investment relationships, including the concerns of American companies; and our commitment to privacy and basic liberties. And we will review decisions about intelligence priorities and sensitive targets on an annual basis so that our actions are regularly scrutinized by my senior national security team.

Second, we will reform programs and procedures in place to provide greater transparency to our surveillance activities, and fortify the safeguards that protect the privacy of U.S. persons. Since we began this review, including information being released today, we have declassified over 40 opinions and orders of the Foreign Intelligence Surveillance Court, which provides judicial review of some of our most sensitive intelligence activities -- including the Section 702 program targeting foreign individuals overseas, and the Section 215 telephone metadata program.

And going forward, I'm directing the Director of National Intelligence, in consultation with the Attorney General, to annually review for the purposes of declassification any future opinions of the court with broad privacy implications, and to report to me and to Congress on these efforts. To ensure that the court hears a broader range of privacy perspectives, I am also calling on Congress to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court.

Third, we will provide additional protections for activities conducted under Section 702, which allows the government to intercept the communications of foreign targets overseas who have information that's important for our national security. Specifically, I am asking the Attorney General and DNI to institute reforms that place additional restrictions on government's ability to retain, search, and use in criminal cases communications between Americans and foreign citizens incidentally collected under Section 702.

Fourth, in investigating threats, the FBI also relies on what's called national security letters, which can require companies to provide specific and limited information to the government without disclosing the orders to the subject of the investigation. These are cases in which it's important that the subject of the investigation, such as a possible terrorist or spy, isn't tipped off. But we can and should be more transparent in how government uses this authority.

I have therefore directed the Attorney General to amend how we use national security letters so that this secrecy will not be indefinite, so that it will terminate within a fixed time unless the government demonstrates a real need for further secrecy. We will also enable communications providers to make public more information than ever before about the orders that they have received to provide data to the government.

This brings me to the program that has generated the most controversy these past few months -- the bulk collection of telephone records under Section 215. Let me repeat what I said when this story first broke: This program does not involve the content of phone calls, or the names of people making calls. Instead, it provides a record of phone numbers and the times and lengths of calls -- metadata that can be queried if and when we have a reasonable suspicion that a particular number is linked to a terrorist organization.

Why is this necessary? The program grew out of a desire to address a gap identified after 9/11. One of the 9/11 hijackers -- Khalid al-Mihdhar -- made a phone call from San Diego to a known al Qaeda safe-house in Yemen. NSA saw that call, but it could not see that the call was coming from an individual already in the United States. The telephone metadata program under Section 215 was designed to map the communications of terrorists so we can see who they may be in contact with as quickly as possible. And this capability could also prove valuable in a crisis. For example, if a bomb goes off in one of our cities and law enforcement is racing to determine whether a network is poised to conduct additional attacks, time is of the essence. Being able to quickly review phone connections to assess whether a network exists is critical to that effort.

In sum, the program does not involve the NSA examining the phone records of ordinary Americans. Rather, it consolidates these records into a database that the government can query if it has a specific lead -- a consolidation of phone records that the companies already retained for business purposes. The review group turned up no indication that this database has been intentionally abused. And I believe it is important that the capability that this program is designed to meet is preserved.

Having said that, I believe critics are right to point out that without proper safeguards, this type of program could be used to yield more information about our private lives, and open the door to more intrusive bulk collection programs in the future. They're also right to point out that although the telephone bulk collection program was subject to oversight by the Foreign Intelligence Surveillance Court and has been reauthorized repeatedly by Congress, it has never been subject to vigorous public debate.

For all these reasons, I believe we need a new approach. I am therefore ordering a transition that will end the

Section 215 bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk metadata.

This will not be simple. The review group recommended that our current approach be replaced by one in which the providers or a third party retain the bulk records, with government accessing information as needed. Both of these options pose difficult problems. Relying solely on the records of multiple providers, for example, could require companies to alter their procedures in ways that raise new privacy concerns. On the other hand, any third party maintaining a single, consolidated database would be carrying out what is essentially a government function but with more expense, more legal ambiguity, potentially less accountability -- all of which would have a doubtful impact on increasing public confidence that their privacy is being protected.

During the review process, some suggested that we may also be able to preserve the capabilities we need through a combination of existing authorities, better information sharing, and recent technological advances. But more work needs to be done to determine exactly how this system might work.

Because of the challenges involved, I've ordered that the transition away from the existing program will proceed in two steps. Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization instead of the current three. And I have directed the Attorney General to work with the Foreign Intelligence Surveillance Court so that during this transition period, the database can be queried only after a judicial finding or in the case of a true emergency.

Next, step two, I have instructed the intelligence community and the Attorney General to use this transition period to develop options for a new approach that can match the capabilities and fill the gaps that the Section 215 program was designed to address without the government holding this metadata itself. They will report back to me with options for alternative approaches before the program comes up for reauthorization on March 28th. And during this period, I will consult with the relevant committees in Congress to seek their views, and then seek congressional authorization for the new program as needed.

Now, the reforms I'm proposing today should give the American people greater confidence that their rights are being protected, even as our intelligence and law enforcement agencies maintain the tools they need to keep us safe. And I recognize that there are additional issues that require further debate. For example, some who participated in our review, as well as some members of Congress, would like to see more sweeping reforms to the use of national security letters so that we have to go to a judge each time before issuing these requests. Here, I have concerns that we should not set a standard for terrorism investigations that is higher than those involved in investigating an ordinary crime. But I agree that greater oversight on the use of these letters may be appropriate, and I'm prepared to work with Congress on this issue.

There are also those who would like to see different changes to the FISA Court than the ones I've proposed. On all these issues, I am open to working with Congress to ensure that we build a broad consensus for how to move forward, and I'm confident that we can shape an approach that meets our security needs while upholding the civil liberties of every American.

Let me now turn to the separate set of concerns that have been raised overseas, and focus on America's approach to intelligence collection abroad. As I've indicated, the United States has unique responsibilities when it comes to intelligence collection. Our capabilities help protect not only our nation, but our friends and our allies, as well. But our efforts will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy, too. And the leaders of our close friends and allies deserve to know that if I want to know what they think about an issue, I'll pick up the phone and call them, rather than turning to surveillance. In other words, just as we balance security and privacy at home, our global leadership demands that we balance our security requirements against our need to maintain the trust and cooperation among people and leaders around the world.

For that reason, the new presidential directive that I've issued today will clearly prescribe what we do, and do not do, when it comes to our overseas surveillance. To begin with, the directive makes clear that the United States only uses signals intelligence for legitimate national security purposes, and not for the purpose of indiscriminately reviewing the emails or phone calls of ordinary folks. I've also made it clear that the United States does not collect intelligence to suppress criticism or dissent, nor do we collect intelligence to disadvantage people on the basis of their ethnicity, or race, or gender, or sexual orientation, or religious beliefs. We do not collect intelligence to provide a competitive advantage to U.S. companies or U.S. commercial sectors.

And in terms of our bulk collection of signals intelligence, U.S. intelligence agencies will only use such data to meet specific security requirements: counterintelligence, counterterrorism, counter-proliferation, cybersecurity, force protection for our troops and our allies, and combating transnational crime, including sanctions evasion.

In this directive, I have taken the unprecedented step of extending certain protections that we have for the American people to people overseas. I've directed the DNI, in consultation with the Attorney General, to develop these safeguards, which will limit the duration that we can hold personal information, while also restricting the use of this information.

The bottom line is that people around the world, regardless of their nationality, should know that the United States is

not spying on ordinary people who don't threaten our national security, and that we take their privacy concerns into account in our policies and procedures. This applies to foreign leaders as well. Given the understandable attention that this issue has received, I have made clear to the intelligence community that unless there is a compelling national security purpose, we will not monitor the communications of heads of state and government of our close friends and allies. And I've instructed my national security team, as well as the intelligence community, to work with foreign counterparts to deepen our coordination and cooperation in ways that rebuild trust going forward.

Now let me be clear: Our intelligence agencies will continue to gather information about the intentions of governments -- as opposed to ordinary citizens -- around the world, in the same way that the intelligence services of every other nation does. We will not apologize simply because our services may be more effective. But heads of state and government with whom we work closely, and on whose cooperation we depend, should feel confident that we are treating them as real partners. And the changes I've ordered do just that.

Finally, to make sure that we follow through on all these reforms, I am making some important changes to how our government is organized. The State Department will designate a senior officer to coordinate our diplomacy on issues related to technology and signals intelligence. We will appoint a senior official at the White House to implement the new privacy safeguards that I have announced today. I will devote the resources to centralize and improve the process we use to handle foreign requests for legal assistance, keeping our high standards for privacy while helping foreign partners fight crime and terrorism.

I have also asked my counselor, John Podesta, to lead a comprehensive review of big data and privacy. And this group will consist of government officials who, along with the President's Council of Advisors on Science and Technology, will reach out to privacy experts, technologists and business leaders, and look how the challenges inherent in big data are being confronted by both the public and private sectors; whether we can forge international norms on how to manage this data; and how we can continue to promote the free flow of information in ways that are consistent with both privacy and security.

For ultimately, what's at stake in this debate goes far beyond a few months of headlines, or passing tensions in our foreign policy. When you cut through the noise, what's really at stake is how we remain true to who we are in a world that is remaking itself at dizzying speed. Whether it's the ability of individuals to communicate ideas; to access information that would have once filled every great library in every country in the world; or to forge bonds with people on other sides of the globe, technology is remaking what is possible for individuals, and for institutions, and for the international order. So while the reforms that I have announced will point us in a new direction, I am mindful that more work will be needed in the future.

One thing I'm certain of: This debate will make us stronger. And I also know that in this time of change, the United States of America will have to lead. It may seem sometimes that America is being held to a different standard. And I'll admit the readiness of some to assume the worst motives by our government can be frustrating. No one expects China to have an open debate about their surveillance programs, or Russia to take privacy concerns of citizens in other places into account. But let's remember: We are held to a different standard precisely because we have been at the forefront of defending personal privacy and human dignity.

As the nation that developed the Internet, the world expects us to ensure that the digital revolution works as a tool for individual empowerment, not government control. Having faced down the dangers of totalitarianism and fascism and communism, the world expects us to stand up for the principle that every person has the right to think and write and form relationships freely -- because individual freedom is the wellspring of human progress.

Those values make us who we are. And because of the strength of our own democracy, we should not shy away from high expectations. For more than two centuries, our Constitution has weathered every type of change because we have been willing to defend it, and because we have been willing to question the actions that have been taken in its defense. Today is no different. I believe we can meet high expectations. Together, let us chart a way forward that secures the life of our nation while preserving the liberties that make our nation worth fighting for.

Thank you. God bless you. May God bless the United States of America. (Applause.)

END  
11:57 A.M. EST

# **EXHIBIT T**

## **IC ON THE RECORD**

- **NEW** [SIGNALS INTEL REFORM REPORT](#)
  - **NEW** [IC Budget](#)
    - [Transparency Reporting](#)
- [Frequently Asked Questions](#)  
[Q&A](#)



### **SIGNALS INTELLIGENCE REFORM**

### **2015 ANNIVERSARY REPORT**

- OVERVIEW
- SEEKING INDEPENDENT ADVICE
- **STRENGTHENING PRIVACY & CIVIL LIBERTIES** «
- LIMITING SIGINT COLLECTION & USE
- ENHANCING TRANSPARENCY
- PROTECTING WHISTLEBLOWERS
- MOVING FORWARD
- FACTSHEET

## **STRENGTHENING PRIVACY & CIVIL LIBERTIES PROTECTIONS**

As the President said in his speech on January 17, 2014, “the challenges posed by threats like terrorism and proliferation and cyber-attacks are not going away any time soon ... and for our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world.” As a part of that effort, the President made clear that “our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside....”

This commitment is reflected in the direction the President issued that same day in Section 4 of Presidential Policy Directive-28, Signals Intelligence Activities (PPD-28), requiring all elements of the Intelligence Community to establish policy and procedures for safeguarding personal information collected from signals intelligence (SIGINT) activities. In addition, we are also seeking to provide new legislative remedies for potential privacy violations.

- **INTELLIGENCE COMMUNITY'S IMPLEMENTATION OF SECTION 4 OF PPD-28**
- **JUDICIAL REDRESS OF CITIZENS OF CERTAIN COUNTRIES**

In addition, in response to the President's direction and to the recommendations from both the President's Review Group on Intelligence and Communications Technology and the Privacy and Civil Liberties Oversight Board, the Intelligence Community is strengthening privacy protections in our collection activities under Section 702 of Foreign Intelligence Surveillance Act and the Section 215 bulk telephony metadata program. Moreover, as directed by the President, the FBI will amend its non-disclosure policy for National Security Letters.

- **NEW PRIVACY PROTECTIONS FOR INFORMATION COLLECTED UNDER SECTION 215**
- **NEW PRIVACY PROTECTIONS FOR INFORMATION COLLECTED UNDER SECTION 702**
- **NATIONAL SECURITY LETTERS**

## **INTELLIGENCE COMMUNITY'S IMPLEMENTATION OF SECTION 4 OF PRESIDENTIAL POLICY DIRECTIVE / PPD-28, SIGNALS INTELLIGENCE ACTIVITIES**

On January 17, 2014, the President issued [Presidential Policy Directive-28](#), Signals Intelligence Activities (PPD-28), which "articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes."

In [a speech that same day](#), the President made clear that the United States is committed to protecting the personal information of all people regardless of nationality and directed the Intelligence Community to take a number of steps to strengthen the privacy and civil liberty protections afforded to all people.

PPD-28 reinforces current practices, establishes new principles, and strengthens oversight, to ensure that in conducting signals intelligence (SIGINT) activities, the United States takes into account not only the security needs of our nation and our allies, but also the privacy of people around the world.

Section 4 of PPD-28 calls on each Intelligence Community element to update existing or issue new policies and procedures to implement principles for safeguarding all personal information collected through SIGINT, consistent with technical capabilities and operational needs.

Over the past year, the Intelligence Community has been working to implement this requirement within the framework of existing processes, resources, and capabilities, while ensuring that mission needs continue to be met.

In July 2014, the Director of National Intelligence provided the President [an interim report on the status of our efforts](#) that also evaluated, in coordination with the Department of Justice and the rest of the Intelligence Community, certain additional retention and dissemination safeguards that all Intelligence Community elements should follow as they adopt policies and procedures under PPD-28.

The Director of National Intelligence is pleased to report that, as required by PPD-28, all Intelligence Community elements have reviewed and updated their existing policies and procedures, or have issued new policies or procedures, to provide safeguards for personal information collected through SIGINT, regardless of nationality and consistent with national security, our technical capabilities, and operational needs.

Although similar in many respects, agency procedures are not identical. The differences reflect that not all agencies conduct SIGINT collection and that agencies have different mission requirements. Links to agency policies and procedures can be found below.

### **U.S. Intelligence Community Policies & Procedures to Safeguard Personal Information Collected Through SIGINT**

- [Office of the Director of National Intelligence](#)
- [Central Intelligence Agency](#)
- [National Security Agency](#)
- [National Reconnaissance Office](#)
- [Federal Bureau of Investigation](#)
- [Department of Homeland Security](#)
- [Drug Enforcement Administration](#)
- [State Department](#)
- [Treasury Department](#)
- [Department of Energy](#)
- [U.S. Coast Guard](#)
- [Other IC Elements in the Department of Defense](#)

### **What has PPD-28 changed?**

The agency policies and procedures implementing Section 4 of PPD-28 include significant changes that strengthen privacy and civil liberty protections for all people. It is worthwhile to highlight a few of the most significant changes:

- **Limits on retention:** We have imposed new limitations on the retention of personal information about non-U.S. persons. Before PPD-28, Intelligence Community elements had disparate restrictions on how long information about non-U.S. persons could be retained. PPD-28 changes these retention practices in significant ways to afford strengthen privacy protections. Now Intelligence Community elements must delete non-U.S. person information collected through SIGINT five years after collection unless the information has been determined to be relevant to, among other things, an authorized foreign intelligence requirement, or if [the Director of National Intelligence determines](#), after considering the views of the Office of the Director of National Intelligence Civil Liberties Protection Officer and agency privacy and civil liberties officials, that continued retention is in the interest of national security. This new retention requirement is similar to the requirements applicable to information about U.S. persons. Thus these new retention rules will more uniformly limit the retention of any personal information by the Intelligence Community.
- **Dissemination Restrictions:** Intelligence Community elements have always disseminated intelligence information because it is relevant to foreign intelligence requirements. All agency policies implementing PPD-28 now explicitly require that information about a person may not be disseminated solely because he or she is a non-U.S. person and the Office of the Director of National Intelligence has issued [a revised directive](#) to all Intelligence Community elements to reflect this requirement. Intelligence Community personnel are now specifically required to consider the privacy interests of non-U.S. persons when drafting and disseminating intelligence reports.
- **Oversight, Training & Compliance Requirements:** Intelligence Community elements have always had strong training, oversight, and compliance programs to ensure we were protecting the privacy and civil liberties of U.S. persons. In response to PPD-28, Intelligence Community elements have added new training, oversight, and compliance requirements. They are developing mandatory training programs to ensure that intelligence officers know and understand their responsibility to protect the personal information of all people, regardless of nationality. We are also adding new oversight and compliance programs to ensure that these new rules are being followed properly. The oversight program includes a new requirement to report any significant compliance incident involving personal information, regardless of the person's nationality, to the Director of National Intelligence.

## JUDICIAL REDRESS FOR CITIZENS OF CERTAIN COUNTRIES

In furtherance of its commitment to protecting privacy in the law enforcement context, the Administration is working with Members of Congress on legislation to give citizens of designated countries the right to seek judicial redress for intentional or willful disclosures of protected information, and for refusal to grant access or to rectify any errors in that information.

## NEW PRIVACY PROTECTIONS FOR BULK TELEPHONY METADATA COLLECTED UNDER SECTION 215



Section 215 of the USA PATRIOT Act authorizes the Government to make requests to the Foreign Intelligence Surveillance Court (FISC) for orders requiring production of documents or other tangible things (books, records, papers, documents, and other items) when they are relevant to an authorized national security investigation such as an investigation to protect against international terrorism or clandestine intelligence activities. The vast majority of orders issued under Section 215 do not seek information collected in bulk; rather, these orders require the production of a discrete and limited amount of information.

This authority is also used to require certain telephone communications providers to produce in bulk telephony metadata, such as telephone numbers dialed and length of calls. This program was developed to fill an important intelligence gap identified by the report on the 9/11 attacks by allowing the Government to detect communications between terrorists who are operating outside the U.S. and potential operatives inside the U.S. This program does not permit the government to obtain or listen to the content of anyone's telephone calls. Nor is the Government allowed to sift indiscriminately through the telephony metadata obtained under this program. Rather, since its inception, this program has been subject to strict controls and oversight, including:

- Requiring the metadata to be stored in secure databases accessible to only a limited number of trained analysts.
- Limiting the access to, and use of, the metadata only for counterterrorism purposes.
- Prohibiting querying the databases unless there is a reasonable, articulable suspicion that a particular target identifier (the "seed" number) is associated with particular foreign terrorist organizations.
- Limiting the access to and use of this metadata only for identifying the telephone identifiers that are in contact, directly or indirectly, with the seed number.
- Destroying the information after five years.

### **New Protections for the Current Program**

In response to the President's direction in January 2014, this program was modified by incorporating into the FISC orders authorizing the bulk collection two forms of enhanced privacy protection:

- Previously, the basis for the reasonable, articulable suspicion finding had to be documented in writing and approved by specifically authorized NSA officials. The Department of Justice conducted routine oversight of these decisions to ensure the standard was met. Today, except in emergency circumstances, reasonable, articulable suspicion findings must also be approved in advance by the FISC. Thus, except in emergency circumstances, only court-approved identifiers may be used to query the database.
- Previously, NSA was permitted to query the information out to three "hops," or links. Today, queries are limited to two hops. This means NSA is permitted to develop contact chains by starting with a target identifier (seed number) and, using telephony metadata records, see what identifiers communicated with that target (first hop) and which identifiers, in turn, communicated with the first-hop identifiers (second hop). The limitation to two hops reduces the number of potential results from each query.

In June 2014, the Office of the Director of National Intelligence released its first annual statistical transparency report on the use of national security authorities covering the year 2013. Later this year, the Director of National Intelligence will issue its second report covering the use of national security authorities in 2014. In advance of that report, it is appropriate to note that in 2014 there were 161 target identifiers approved by the FISC to be queried under NSA's bulk telephony metadata program.

### **New Protections to be Established by Legislation**

In his January 17, 2014 speech, the President directed the Department of Justice and the Intelligence Community to develop options for a new approach that would match the capabilities and fill the gaps that Section 215 was designed to address without the government holding the metadata itself. The Department of Justice and the Intelligence Community explored a number of options, including having the metadata held by a third party or leaving the metadata at the provider.

Based on recommendations from the Department of Justice and the Intelligence Community, the President proposed that the government end bulk collection of telephony metadata under Section 215 of the USA PATRIOT Act, while ensuring that the government has access to the information it needs to meet its national security requirements. The Intelligence Community and the Department of Justice have since been working closely with Congress to develop legislation that would implement the President's proposal by leaving the metadata at the provider.

To that end, the Administration supported the USA FREEDOM Act, which, if enacted, would have prohibited bulk collection using (i) Section 215, (ii) the Pen Registers and Trap and Trace provisions of the Foreign Intelligence Surveillance Act, and (iii) National Security Letters while maintaining critical authorities to conduct more targeted collection.

The Attorney General and the Director of National Intelligence stated that, based on communications providers' existing data retention practices, the bill would retain the essential operational capabilities of the existing bulk telephone metadata program while eliminating bulk collection by the government under these legal authorities. The bill would also expressly authorize an independent voice in significant cases before the FISC.

The Administration was disappointed that the 113th Congress ended without enacting this legislation. This legislation not only satisfies the President's requirements, but also responds to the recommendations from the Privacy and Civil Liberties Oversight Board and the President's Review Group on Intelligence and Communications Technology to end the bulk collection of telephony metadata records under Section 215 of USA PATRIOT Act as it currently exists.

The Intelligence Community encourages Congress to quickly take up and pass legislation that would allow the government to end bulk collection of telephony metadata records under Section 215, while ensuring that the government has access to the information it needs to meet its national security requirements.

## **NEW PRIVACY PROTECTIONS FOR INFORMATION COLLECTED UNDER SECTION 702**

Section 702 of the Foreign Intelligence Surveillance Act (FISA), which was added by the FISA Amendments Act of 2008, authorizes the acquisition of foreign intelligence information concerning non-U.S. persons reasonably believed to be located outside the United States.

Under Section 702, the government cannot target anyone for collection unless it has a significant purpose to acquire foreign intelligence information, the foreign target is reasonably believed to be outside the United States, and the Government abides by FISC-approved targeting and minimization procedures.

Section 702 cannot be used to intentionally target any U.S. citizen or any other U.S. person, to intentionally target any person known to be in the United States, or to target a person outside the United States if the purpose is to target a person inside the United States.

Collection under Section 702 does not require individual judicial orders authorizing collection against each target. Instead, Section 702 requires that the FISC approve procedures to (i) ensure that only non-U.S. persons reasonably believed to be outside the U.S. are targeted, and (ii) minimize the acquisition, retention, and dissemination of incidentally acquired information about U.S. persons.

Activities authorized by Section 702 are subject to oversight by the Judicial Branch through the Foreign Intelligence Surveillance Court, by the Executive Branch through the Department of Justice and the Office of the Director of National Intelligence, and by the Legislative Branch through the Intelligence and Judiciary Committees of Congress. Directives requiring the production of information to the Government can be challenged in the FISC by the recipients.

In his January 17, 2014 address, the President asked the Department of Justice and the Intelligence Community to institute reforms with respect to the government's ability to retain, search, and use in criminal cases communications between Americans and foreign citizens incidentally collected under Section 702.

Subsequently, in July 2014, the [Privacy and Civil Liberties Oversight Board issued a report on Section 702](#), concluding that the Section 702 program is lawful and valuable, and that "at its core, the program is sound" and making ten recommendations to help the program "strike a better balance between privacy, civil rights, and national security."

As noted above, in response to the President's direction and recommendations from the Privacy and Civil Liberties Oversight Board, the Attorney General and Director of National Intelligence are placing additional restrictions on the government's ability to retain, query, and use in evidence in criminal proceedings communications between Americans and foreign citizens incidentally collected under Section 702.

- First, FBI, CIA, and NSA each are instituting new requirements for using a U.S. person identifier to query information acquired under Section 702. As recommended by the Privacy and Civil Liberties Oversight Board, NSA's minimization procedures will require a written statement of facts showing that a query is reasonably likely to return foreign intelligence information. CIA's minimization procedures will be similarly amended to require a statement of facts for queries of content. In addition, FBI's minimization procedures will be updated to more clearly reflect the FBI's standard for conducting U.S. person queries and to require additional supervisory approval to access query results in certain circumstances.
- Second, the new policy re-affirms requirements that the government must delete communications to, from, or about U.S. persons acquired under Section 702 that have been determined to lack foreign intelligence value. In addition, the policy requires the Department of Justice and the Office of the Director of National Intelligence to conduct oversight over these retention decisions. This change will help ensure that the Intelligence Community preserves only that information that might help advance its national security mission.
- Third, consistent with the recommendation of the Privacy and Civil Liberties Oversight Board, information acquired under Section 702 about a U.S. person will not be introduced as evidence against that person in any criminal proceeding except (1) with the approval of the Attorney General, and (2) in criminal cases with national security implications or certain other serious crimes. This change will ensure that, if the Department of Justice decides to use information acquired under Section 702 about a U.S. person in a criminal case, it will do so only for national security purposes or in prosecuting the most serious crimes.

The Intelligence Community has also agreed to address the Privacy and Civil Liberties Oversight Board's other recommendations, including:

- Revising targeting procedures to require additional documentation of the foreign intelligence value of each target;
- Making available to the FISC additional information to help the Court evaluate the annual certifications in support of collection under Section 702;
- Initiating studies to ensure that the Intelligence Community is using the best filtering technology and techniques to prevent inadvertent collection;
- Publicly releasing the minimization procedures of the [CIA](#), [NSA](#), and the [FBI](#);
- Evaluating whether NSA can track and publicly release additional statistics on its collection and use of information obtained pursuant to Section 702;
- Supporting the Privacy and Civil Liberties Oversight Board's ongoing effort examine efforts across the Intelligence Community to assess the efficacy and relative value of counterterrorism programs.

## **NATIONAL SECURITY LETTERS**

A National Security Letter is an investigative tool, similar to a subpoena, which is used by the FBI in a national security-related investigation to obtain limited types of information from companies, such as telephone records and subscriber information.

When the FBI issues a National Security Letter, by law a senior official, such as the Special Agent in Charge of a field office, may require that the recipient company not disclose the existence of the letter, if one or more statutory standards are met – that is, when disclosure may (i) endanger the national security of the United States, (ii) interfere with a criminal, counterterrorism or counterintelligence investigation, (iii) interfere with diplomatic relations, or (iv) endanger the life or physical safety of any person.

In his January 17, 2014 remarks, the President directed the Attorney General “to amend how we use National Security Letters so that [their] secrecy will not be indefinite, and will terminate within a fixed time unless the government demonstrates a real need for further secrecy.”

In response to the President’s new direction, the FBI will now presumptively terminate National Security Letter nondisclosure orders at the earlier of three years after the opening of a fully predicated investigation or the investigation’s close.

Continued nondisclosures orders beyond this period are permitted only if a Special Agent in Charge or a Deputy Assistant Director determines that the statutory standards for nondisclosure continue to be satisfied and that the case agent has justified, in writing, why continued nondisclosure is appropriate.

[Back to Top](#)

## IC ON THE RECORD:

Direct access to factual information related to the lawful foreign surveillance activities of the U.S. Intelligence Community.

Created at the direction of the President of the United States and maintained by the Office of the Director of National Intelligence.

Follow @IContheRecord

---

### CONTENT:

- - [Official Statements](#)
- - [Declassified Documents](#)
- - [Testimony](#)
- - [Speeches & Interviews](#)
- - [Fact Sheets](#)
- - [Oversight & Compliance](#)
- - [Video](#)

---

### HOT TOPICS:

- - [Civil Liberties](#)
- - [FISA](#)
- - [FISC](#)
- - [Section 215](#)
- - [Section 702](#)

---

### THEIR OWN WORDS:

- - [James Clapper, DNI](#)
- - [Mike Rogers, Dir. NSA](#)
- - [Rick Ledgett, Dep. Dir. NSA](#)
- - [Robert Litt, GC, ODNI](#)
- - [Rajesh De, GC, NSA](#)
- - [Alex Joel, CLPO, ODNI](#)
- - [Becky Richards, CLPO, NSA](#)
- - [John DeLong, CD, NSA](#)

### (Former IC Officials)

- - [Keith Alexander, Dir. NSA](#)
- - [John Inglis, Dep. Dir. NSA](#)

Search this site



This website is maintained by the [Office of the Director of National Intelligence](#).