NATIONAL SECURITY LETTERS REFORM ACT OF 2007

HEARING

BEFORE THE

SUBCOMMITTEE ON THE CONSTITUTION, CIVIL RIGHTS, AND CIVIL LIBERTIES

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

ON

H.R. 3189

APRIL 15, 2008

Serial No. 110–96

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE
41–795 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SÁNCHEZ, California
STEVE COHEN, Tennessee
HANK JOHNSON, Georgia
BETTY SUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota
LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

PERRY APELBAUM, *Staff Director and Chief Counsel*
SEAN MCLAUGHLIN, *Minority Chief of Staff and General Counsel*

SUBCOMMITTEE ON THE CONSTITUTION, CIVIL RIGHTS, AND CIVIL LIBERTIES

JERROLD NADLER, New York, *Chairman*

ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota
JOHN CONYERS, JR., Michigan
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
STEVE COHEN, Tennessee
TRENT FRANKS, Arizona
MIKE PENCE, Indiana
DARRELL ISSA, California
STEVE KING, Iowa
JIM JORDAN, Ohio

DAVID LACHMANN, *Chief of Staff*
PAUL B. TAYLOR, *Minority Counsel*

CONTENTS

APRIL 15, 2008

NATIONAL SECURITY LETTERS REFORM ACT OF 2007

TUESDAY, APRIL 15, 2008

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON THE CONSTITUTION,
CIVIL RIGHTS, AND CIVIL LIBERTIES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 1:12 p.m., in Room 2141, Rayburn House Office Building, the Honorable Jerrold Nadler (Chairman of the Subcommittee) presiding.

Present: Representatives Conyers, Nadler, Wasserman Schultz, Ellison, Scott, Watt, and Franks.

Staff present: David Lachmann, Subcommittee Chief of Staff; Robert Reed, Majority Counsel; Carole Angel, Majority Legislative Assistant; Caroline Mays, Majority Professional Staff Member; Paul B. Taylor, Minority Counsel; and Jennifer Burba, Minority Staff Assistant.

Mr. NADLER. This hearing of the Subcommittee on the Constitution, Civil Rights, and Civil Liberties will come to order.

Welcome, everyone.

Without objection, the Chair is authorized to declare a recess, which the Chair will do when they call votes on the floor.

The Chair will recognize himself now for 5 minutes for an opening statement.

Today's hearing focuses on the law governing National Security Letters, the widespread abuses of the authority given to the FBI to issue NSLs is documented in two reports by the Department of Justice's Inspector General, and proposed legislation to address these threats to the liberty and privacy of law-abiding Americans.

A National Security Letter can be issued to a third party, such as a health insurance company or an Internet service provider, ordering it to reveal all the information in its possession about you and your communications, your transactions or the books you read. The third party is prohibited from telling you or anyone else, aside from the attorney or those processing the information, about the order.

So, you cannot object to the NSL in court, as you could to a subpoena, because you do not know about it. And the third party may have no interest in going to court to protect your rights.

In fact, we invited many of these third parties here today to testify, but they were gagged from disclosing that they had received

NSL requests and were chilled from engaging in this important debate, which directly impacts both them and the general public.

When we debated the reauthorization of the PATRIOT Act a few years ago, Congress and the public was not yet aware of the extent of the abuses brought about by the FBI's overuse of NSLs outside the bounds of their proper authority.

Indeed, even the changes made to the NSL provisions by the 2005 PATRIOT Act Reauthorization Act were, for all practical purposes, meaningless. For example, the court is authorized by the 2005 amendment to modify or set aside the gag order, if it finds there is no reason to believe that disclosure would endanger national security, diplomatic relations or anyone's life or safety.

But the court must accept the government's assertion of such harm as conclusive and cannot use its own judgment as to whether, in fact, such harm would result. Since the government's assertion is conclusive, there is no room for the court at all, and the provision is meaningless.

In addition, the burden remains on the recipient of the NSL to challenge the order. This would seem to violate the first amendment's heavy burden of proof against prior restraints of publication.

When these provisions were first debated, some of us had predicted that the unrestricted authority of the FBI to issue NSLs would be abused. Unfortunately, these fears have been realized. The I.G.'s audit (INAUDIBLE) the NSLs have been used by the FBI to collect and retain private information about American citizens who are not reasonably suspected of being involved in terrorism.

That is why I have introduced, along with a number of others, the bipartisan National Security Letters Reform Act of 2007. This legislation will protect Americans against unnecessary and unsupported intrusions into their private lives and, more importantly, should prevent abuse of power by the government. We need to fix the law to bring it in line with the Constitution, to enhance checks and balances, and in doing so, to better protect our national security.

Already, courts have found parts of the NSL authority to be too broad and unconstitutional. The provisions that state the NSL recipients are forbidden from disclosing the demand to the targeted individual or to almost anyone else but their attorney, has already been struck down as a prior restraint, repugnant to the first amendment. Another Federal court found the NSL authority to be unconstitutional, because it violates the fourth amendment's protection against unreasonable searches and seizures.

The bipartisan bill that I am the lead co-sponsor of would lawfully authorize intelligence agencies to use NSLs with proper safeguards.

Specifically, it:

Would restore the standard that the records sought pertain to a suspected terrorist or spy;

Would give an NSL recipient the right to challenge the letter and its non-disclosure requirement—a real right to challenge, not one in which the government's assertion is dispositive—to place a time

limit on the gag order and allow for court-approved extensions of that time limit;

Would provide a course of action to any person aggrieved by the illegal provision of records pertaining to that person as the result of an NSL issued contrary to law, or of an NSL issued, based on the certification made without factual foundation;

Would give notice to the target of an NSL if the government seeks to use the records obtained from the NSL in a subsequent proceeding;

Would give the target an opportunity to receive legal counsel and challenge the use of those records in such a subsequent proceeding;

Would provide for minimization procedures to ensure that information obtained pursuant to an NSL regarding persons that are no longer of interest in an authorized investigation is destroyed; and

Would address the voluntary disclosure of customer communications or records that had been obtained through so-called "exigent" letters.

I do not think it is too much to ask the FBI to follow the Constitution and the rule of law while it goes about its job of protecting us. The abuses of power by the DOJ and the FBI show that legislative fixes are needed to check the over-broad and unchecked investigatory power.

By requiring that NSLs be issued only if the FBI has made a factual, individualized showing that the directive sought to obtain to a suspected terrorist or spy, we will help keep our law enforcement focused on real threats.

The time for this over-broad power to be curtailed is now, and I am hopeful that we will be successful. The abuses by the DOJ and the FBI have proven that these legislative fixes are a necessary check on the investigatory power.

Just today, the Electronic Frontier Foundation, EFF, disclosed that documents obtained by the EFF through a Freedom of Information Act request showed a misuse of the FBI's National Security Letter authority, issued at the direction of FBI headquarters went unreported to the Intelligence Oversight Board for almost 3 years.

Self-policing has proven time and again to be both undemocratic and ineffective. It is not enough to mandate that the FBI fix internal management problems and record keeping, because the statute itself authorizes the unchecked collection of information of innocent Americans. Congress should act now to fix the underlying statutes authorizing this unconstitutional and unchecked authority, which has led to the abuses revealed in the I.G. report, and to hold those responsible for these violations accountable.

We must have intelligence gathering. We need our safety. But we must do our intelligence gathering under constitutional and legal checks to protect our privacy and our liberties, as well as our safety.

I want to welcome our witnesses. I look forward to their testimony.

I yield back the balance of my time, and I now recognize the distinguished Ranking minority Member of the Committee, the gentleman from Arizona, Mr. Franks, for 5 minutes for an opening statement.

Mr. FRANKS. Well, thank you, Mr. Chairman.

Mr. Chairman, the bill that we address today at this hearing, H.R. 3189, would, in my sincere judgment, render National Security Letters as ineffective as they were prior to 9/11, and would further squelch the initiation of vital terrorism investigations. By changing the standards for such terrorism investigations, the bill would preclude many investigations that would otherwise be able to go forward, and would do so in a manner directly contrary to the findings of two recent Inspector General's reports and the 9/11 Commission, which counseled against returning to the investigative model that failed before the 9/11 attack.

H.R. 3189 would also provide the subjects of terrorism investigations with more protections than they enjoy by even ordinary domestic American criminals under the clear Supreme Court precedents, such as the *United States v. Miller*, that hold that no fourth amendment protections apply to business records handed over to a third party.

The FBI has testified as follows: "National security letters generally permit us to obtain the same sort of documents from third party businesses that prosecutors and agents obtain in a criminal investigation with grand jury subpoenas. National security letters have been instrumental in breaking up cells like the Lackawanna Six and the Northern Virginia Jihad, through the use of NSLs, the FBI has traced sources of terrorist funding, established telephone linkages that resulted in further investigations and arrests, and arrests of suspicious associates with deadly weapons and explosives. NSLs also allow the FBI to link terrorists together financially and pinpoint cells and operatives by following the money."

According to the Inspector General's first report on NSLs, issued in March 2007, NSLs were not an effective means of preventing terrorist attacks before the 9/11 attacks, because "prior to the PATRIOT Act, agents could seek National Security Letters for telephone and electronic communication transactional records from telephone companies and Internet service providers, records from financial institutions and information from credit bureaus, only upon demonstrating 'specific and articulable facts' giving reason to believe that the subject was 'an agent of a foreign power.' FBI agents told us that this prediction standard limited the utility of NSLs as an investigative tool. FBI field and headquarters personnel who have worked with National Security Letters before and after the PATRIOT Act believe that their use and effectiveness has significantly increased after the PATRIOT Act was enacted."

FBI headquarters and field personnel told the Inspector General that they found National Security Letters to be indispensable for "our bread and butter."

Mr. Chairman, H.R. 3189 would dramatically stem the flow of information throughout the investigative process by effectively precluding their availability before the very first steps can be taken down an investigatory trail.

On the video screens right now, there is a diagram from the Inspector General's report that shows all of us the investigative process that would be halted, were National Security Letters' authorizations limited, from requests for FISA warrants to the general intelligence reports to be shared with other agencies.

The Inspector General report that information derived from National Security Letters "most often is used for intelligence purposes rather than for criminal investigation." Yet H.R. 3189 would impose the failed model based on criminal prosecutions alone that failed to prevent the 9/11 attacks.

As the 9/11 Commission itself concluded, "The law enforcement process is concerned with proving the guilt of persons apprehended and charged. It was not designed to ask if the events might be harbingers of worse things to come. Nor did it allow for aggregating and analyzing facts to see if they could provide clues to terrorist tactics more generally."

Mr. Chairman, the Inspector General's report issued in March 2008 concluded that, while some irregularities remained in the administration of National Security Letters, the FBI had made great progress in implementing procedures that will correct errors before they are made. So, oversight has been successful.

And I just want to add, it is commonplace to hear critics of national security programs to quote Benjamin Franklin as saying, "If we surrender our liberties in the name of security, we shall have neither."

Mr. Chairman, those are not Mr. Franklin's actual words. Accurately quoted, Mr. Franklin's words are much more revealing. Ben Franklin wrote these words. He said, "Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety."

H.R. 3189 would protect no essential liberties, and it would significantly weaken national security. And I am hoping, Mr. Chairman, that along with several other bills that have been before this Committee that seem to protect terrorists more than American citizens, that we can somehow get past this.

And with that, I yield back.

Mr. NADLER. The gentleman yields back, and I thank the gentleman.

Without objection, other Members' opening statements will be included in the record.

We have two distinguished panels of witnesses today.

Our first witness is Glenn Fine, the Inspector General for the Department of Justice, since December 15, 2000. Mr. Fine has worked at the Department of Justice of the Inspector General since—or the Inspector General of the Department of Justice—since January 1995. Initially, he was special counsel to the I.G. In 1996, he became the director of the Office of Inspector General, Special Investigations and Review Unit.

Before joining the Office of Inspector General, Mr. Fine was an attorney specializing in labor and employment law at a law firm in Washington, D.C. Prior to that, from 1986 to 1989, Mr. Fine served as assistant U.S. attorney in the Washington, D.C., U.S. Attorney's Office.

He holds an A.B. from Harvard College, a B.A. and M.A. degrees from Oxford University—I think the first person I have seen with two B.A. degrees, an A.B. and a B.A.—and a law degree from Harvard Law School.

Valerie Caproni has served as the general counsel for the Federal Bureau of Investigation since August of 2003. She holds a B.A.

from Newcomb College at Tulane University and a law degree from the University of Georgia.

Ms. Caproni clerked for the Honorable Phyllis Kravitch, United States Court of Appeals, 11th Circuit; was an assistant U.S. attorney in the Criminal Division of the U.S. Attorney's Office, Eastern District of New York; and a general counsel to the New York State Urban Development Corporation—a very challenging job.

She served as Chief of Special Prosecutions and Chief of the Organized Crime and Racketeering Section before becoming Chief of the Criminal Division in 1994. As chief of the Criminal Division, she supervised approximately 100 assistant U.S. attorneys.

Ms. Caproni remained chief of the Criminal Division until she departed in 1998, to become the regional director of the Pacific regional office of the Securities and Exchange Commission.

I would note with some regret that we did not receive Ms. Caproni's testimony prior to the hearing. We do try to show some flexibility to our witnesses in recognition of the fact that their assistance to the Committee is work—but the rule that we should get the testimony in advance exists for a reason. Members do read the testimony ahead of time to prepare for these hearings. It is especially important, because the witnesses make only a 5-minute statement summarizing their written testimony.

This is not a new issue for the Bureau or for the Administration. The Bureau has commented on the I.G.'s findings and provided testimony in the past. I am at a loss to understand why the Bureau was unable to provide the testimony in advance.

In view of the importance of the issue and the importance of Ms. Caproni's testimony, I will allow her to proceed. But I must say that the Administration has too often refused to provide this Committee with answers to appropriate questions, documents necessary to our work, and in many instances refused to provide a legal basis for doing so.

I do not take this conduct lightly. I hope that Ms. Caproni will take back to the Bureau and to the Administration the Committee's frustration with the seeming inability or unwillingness to cooperate in our work.

The rights of all Americans at stake in this matter are great, and I do not appreciate the investigation being treated in a cavalier manner.

Without objection, the written statements of the witnesses will be made part of the record in their entirety.

We would ask each of you to summarize your testimony in 5 minutes or less. To help you keep time, there is a timing light at your table. When 1 minute remains, the light will switch from green to yellow, and then to red when the 5 minutes are up.

Before we begin, it is customary for the Committee to swear in its witnesses.

If you could please stand and raise your right hand to take the oath.

Do you swear or affirm under penalty of perjury that the testimony you are about to give is true and correct, to the best of your knowledge, information and belief?

Thank you.

Let the record reflect that the witnesses answered in the affirmative, and you may be seated.

I will now recognize Mr. Fine for 5 minutes.

TESTIMONY OF GLENN A. FINE, INSPECTOR GENERAL, OFFICE OF THE INSPECTOR GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. FINE. Mr. Chairman, Ranking Member Franks and Members of the Subcommittee, thank you for inviting me to testify about the Office of the Inspector General's recent reports on the FBI's use of National Security Letters and Section 215 orders.

Over the last 2 years, the OIG has issued two sets of reports on these subjects. Our first two reports, issued in March 2007, found widespread and serious misuse of National Security Letters. Last month, as required by the PATRIOT Reauthorization Act, we completed two follow-up reports, which assessed the use of National Security Letters in 2006, the FBI's response to our first report and the FBI's use of Section 215 orders.

First, however, I would like to thank the OIG staff who worked on these reports for their outstanding efforts. The three leaders of the team—Roslyn Mazer, Mara Lee, and Michael Gulledge—are with me here today, and I would like to thank them for their work.

My written statement details the findings of our two recent reports. In my oral statement today, I will briefly highlight some of these findings.

First, our recent report on National Security Letters, NSLs, concluded that the FBI and the department have made significant progress in implementing the recommendations contained in our first report and in adopting other corrective actions. We found that the FBI has devoted substantial time, energy and resources toward seeking to ensure that its field managers and agents understand the seriousness of the FBI's shortcomings and their responsibility for correcting these deficiencies.

Among the actions that the FBI has taken include: developing a new data system to facilitate issuance and tracking of NSLs and to improve the accuracy of required data in congressional and public reports; issuing numerous guidance memoranda and providing mandatory training to FBI employees on the proper use of NSLs; and prohibiting the use of exigent letters.

The FBI also has created a new Office of Integrity and Compliance, modeled after private sector compliance programs. In addition, the department's National Security Division is conducting reviews to examine whether the FBI is using various intelligence techniques, including NSLs, in accordance with applicable laws, guidelines and policies.

Yet, while the FBI and the department have taken positive steps, we also concluded that additional work remains to be done. For example, a department working group was directed to examine how NSL-derived information is used and retained by the FBI. We concluded that the working group's initial proposal did not adequately address measures to label or tag NSL-derived information or to minimize the retention and dissemination of such information.

Our report also notes that the FBI still needs to address or fully implement several other key recommendations, such as reevalu-

ating the reporting structure for the chief division counsel in each FBI field office.

As required by the PATRIOT Reauthorization Act, our recent report also reviewed the FBI's use of NSLs in 2006, which, it is important to note, is a period before our first NSL report was issued in 2007.

Our recent report found a continued upward trend in the use of NSLs, with 49,000 requests in 2006—a 4.7 percent increase from the previous year. The percentage of NSL requests that related to investigations of U.S. persons also continued to increase, to approximately 60 percent.

We also examined the FBI's own reviews of field case files, which found a rate of NSL violations, 9.4 percent, that was even higher than what we found, 7.5 percent.

The number of possible intelligence violations identified by the field reviews was 640, which is a substantial number. Moreover, in 2006, the number of violations reported by FBI field offices was significantly higher than the number of reported violations in prior years.

Our recent review also found that 97 percent of the NSLs in 2006 imposed non-disclosure and confidentiality requirements.

It is also important to note that the most serious violations involving the use of NSL authorities in 2006 relate to the FBI's use of so-called exigent letters, a practice by which the FBI improperly obtained telephone toll billing records from three communication service providers without first issuing NSLs.

The OIG is in the process of completing a separate investigation examining the use of these exigent letters, as well as the use of "blanket NSLs" and other improper requests for telephone records. Among other things, our upcoming report will assess the accountability of FBI personnel for these practices.

As to our follow-up report on Section 215 orders, we found that FBI agents continued to encounter processing delays for obtaining these orders. The average processing time for such orders was 147 days.

We did not identify any illegal use of Section 215 orders in 2006. However, our report discusses one case in which the FISA Court twice refused to authorize a Section 215 order, because of concerns that the investigation was based on protected first amendment activity. However, we found that the FBI subsequently issued NSLs to obtain information about the subject based on the same factual predicate.

In conclusion, we believe the FBI has evidenced a commitment to correcting the serious problems we found in our first report on National Security Letters and has made significant progress in addressing the need to improve compliance in the FBI's use of NSLs. However, the FBI and the department's corrective measures are not yet fully implemented, and we believe it is too early to determine whether these measures will fully eliminate the problems we found with the use of these authorities.

That concludes my prepared statement, and I would be pleased to answer any questions.

[The prepared statement of Mr. Fine follows:]

PREPARED STATEMENT OF GLENN A. FINE

Mr. Chairman, Ranking Member Franks, and Subcommittee Members:

Thank you for inviting me to testify about the Office of the Inspector General's (OIG) recent reports on the Federal Bureau of Investigation's (FBI) use of national security letters (NSL) and Section 215 orders to obtain business records.

The Patriot Reauthorization Act of 2005 (Reauthorization Act) directed the OIG to review the FBI's use of NSLs and Section 215 orders in two separate time periods. The OIG's first reports, issued in March 2007, examined the FBI's use of NSLs from 2003 through 2005, and its use of 215 orders from 2002 through 2005.

As required by the Reauthorization Act, last month the OIG issued two follow-up reports that examined the use of these authorities in 2006. In addition, our follow-up report on national security letters examined the measures taken or proposed by the FBI and the Department of Justice (Department) to address the serious misuse of national security letters that our first NSL report detailed.

In this written statement, I summarize the findings of the two reports that we issued last month. I first discuss the findings regarding the FBI's and the Department's corrective actions to address the serious deficiencies we described in last year's NSL report. I then summarize the findings regarding the FBI's use of NSLs in 2006. Finally, I summarize our report on the FBI's use of Section 215 orders in 2006.

I. NATIONAL SECURITY LETTERS

To conduct the follow-up review on the FBI's use of NSLs that we issued last month, the OIG interviewed FBI personnel at Headquarters and in FBI field offices, and Department personnel in the National Security Division and the Office of the Chief Privacy and Civil Liberties Officer. We analyzed more than 18,000 documents, including NSL-related guidance and training materials developed by the FBI since our first NSL report. OIG personnel also observed the FBI's new data system designed to manage and track NSLs, and they visited three FBI field offices to assess the accuracy of the FBI's review of NSLs issued by those offices. In particular, the OIG re-examined case files that had been reviewed by FBI inspectors and compared our findings to the FBI's findings. We also analyzed data in the FBI's NSL tracking database and examined the Department's annual public reports and the Department's semiannual classified reports to Congress to evaluate NSL requests in 2006 and trends in NSL usage. The following sections summarize the findings in our follow-up report based on this work.

A. Corrective Actions Implemented or Proposed Since our March 2007 NSL Report

Our review concluded that the FBI and the Department have made significant progress in implementing the recommendations contained in our first NSL report and in adopting other corrective actions to address the serious problems we identified in the FBI's use of NSLs. We also found that the FBI has devoted substantial time, energy, and resources toward ensuring that its field managers and agents understand the seriousness of the FBI's shortcomings in its use of NSLs and their responsibility for correcting these deficiencies.

Our interviews of senior FBI officials found that the FBI's leadership is committed to correcting the serious deficiencies in the FBI's use of NSLs identified in our first report. In addition, the FBI's leadership has attempted to reinforce throughout the FBI the necessity for adhering to the rules governing the use of NSL authorities.

We determined that the FBI has taken a variety of actions to address the deficiencies in its use and oversight of NSLs since issuance of our March 2007 report. The actions include:

- Developing a new NSL data system to facilitate issuance and tracking of NSLs and improve the accuracy of data on NSL usage in required congressional and public reports;
- Issuing numerous NSL policies and guidance memoranda and providing mandatory training to FBI employees on the proper use of NSLs; and
- Prohibiting the use of exigent letters.

The FBI has also created a new Office of Integrity and Compliance (OIC), modeled after private sector compliance programs, to seek to ensure that national security investigations and other FBI activities are conducted in a manner consistent with appropriate laws, guidelines, regulations, and policies. We believe this office can perform a valuable function by providing a process for identifying compliance requirements and risks, assessing existing FBI control mechanisms, and developing and implementing better controls to ensure proper use of NSLs. However, we recommend that the FBI consider providing the OIC with a larger permanent staffing

level so that the OIC can develop the skills, knowledge, and independence to lead or directly carry out the critical elements of this new compliance program.

Our report also noted that the Department's National Security Division has implemented additional measures to promote better compliance with NSL authorities and to address other issues raised by our first report. For example, in 2007 the National Security Division began reviews to examine whether the FBI is using various intelligence techniques—including NSLs—in accordance with applicable laws, guidelines, and policies.

Yet, while the FBI and the Department have taken positive steps to address the issues that contributed to the serious misuse of NSL authorities we described in our March 2007 report, we concluded that additional work remains to be done. For example, in response to the recommendations in our 2007 NSL report, the Department's Office of the Chief Privacy and Civil Liberties Officer convened a working group to examine how NSL-derived information is used and retained by the FBI, with special emphasis on the protection of privacy interests. Our assessment of the working group's initial proposal that was completed in August 2007 but subsequently withdrawn is that the proposal did not adequately address measures to label or tag NSL-derived information or to minimize the retention and dissemination of such information. In our recent report, we recommended that the working group consider further whether and how to provide additional privacy safeguards and measures for minimizing the retention of NSL-derived information.

In addition, our report notes that the FBI still needs to address or fully implement several of the key recommendations in our March 2007 report. For example, we recommended that the FBI address our concern about the reporting chain of Chief Division Counsels (CDCs), the chief lawyers in each FBI field office. Based on our concerns that some CDCs were reluctant to provide an independent legal review of NSLs for fear of second-guessing or antagonizing the Special Agents in Charge to whom they report, our recommendation was designed to ensure that CDCs provide close and independent review of NSL requests. While we recognize that the reporting chain of CDCs is an issue that affects many aspects of the CDCs' role and not just their approval of NSLs, we believe the FBI should address and resolve this important issue in a timely manner.

Our report also analyzed three NSL reviews conducted by the FBI following release of our first NSL report in March 2007. One of the FBI reviews examined the use of NSLs in a random sample of 10 percent of counterterrorism, counterintelligence, and foreign computer intrusion cyber investigation case files active in FBI field offices between 2003 and 2006. The FBI's 10 percent review confirmed the types of deficiencies and possible intelligence violations in the FBI's use of NSLs that we identified in our first report. In fact, the FBI's statistically valid sample of field case files found a rate of NSL violations (9.43 percent) higher than what we found (7.5 percent) in the non-statistical sample of NSLs we examined in our first report.

Moreover, when we independently examined the FBI's 10-percent field review in detail, we determined that it did not identify all NSL-related possible intelligence violations and therefore does not provide a fully reliable baseline from which to measure future FBI compliance with NSL authorities. In addition, because the FBI was unable to locate information provided in response to a significant number of NSLs chosen for review in its sample, the results of the FBI field review likely understated the rate of possible intelligence violations.

The FBI's reviews also confirmed two of the most significant findings in our first NSL report. First, the reviews confirmed that the FBI's use of NSLs resulted in many intelligence violations. For example, the FBI's 10 percent review of field office NSLs found at least 640 potential intelligence violations from 2003 through 2006. Extrapolating the results of the FBI's 10 percent statistical sample to the full number of NSLs means that the total number of possible intelligence violations among all NSLs issued over the 4-year period could be as high as 6,400.

Second, the FBI's reviews confirmed that the FBI's internal policies requiring reports to FBI Headquarters of possible NSL-related intelligence violations had not been effective. For example, less than 2 percent of the possible intelligence violations identified by FBI inspectors in the 2007 field review previously had been reported to FBI Headquarters as required.

In short, our review of the FBI's corrective actions concluded that the FBI and the Department have evidenced a commitment to correcting the serious problems we found in our first NSL report and have made significant progress in addressing the need to improve compliance in the FBI's use of the NSLs. However, because only 1 year has passed since our first NSL report in March 2007, and because some measures are not fully implemented or tested, we believe it is too early to definitively state whether the new systems and controls developed by the FBI and the

Department will eliminate fully the problems with NSLs that we identified. We believe the FBI must implement all of our recommendations in our first NSL report, demonstrate sustained commitment to the steps it has taken and committed to take to improve compliance, implement the additional recommendations described in our follow-up report, consider additional measures to enhance privacy protections for NSL-derived information, and remain vigilant in holding FBI personnel accountable for properly using and approving NSLs and for handling responsive records appropriately.

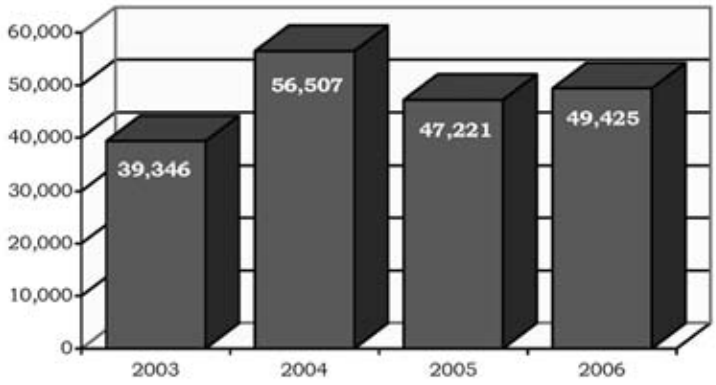
B. Use of National Security Letters in 2006

As required by the Patriot Reauthorization Act, we also reviewed the FBI's use of NSLs in 2006. As discussed in our report, under five statutory provisions the FBI can use NSLs to obtain records such as toll billing records and subscriber information from communication service providers, transactional records from Internet service providers, bank records from financial institutions, and full or limited consumer credit information from credit reporting agencies. The Patriot Act broadened the FBI's authority to use NSLs by lowering the threshold standard for issuing NSLs, allowing FBI field office Special Agents in Charge to sign NSLs, and permitting the FBI to use NSLs to obtain full credit reports in international terrorism investigations.

First, it is important to note that the FBI's use of NSLs in 2006 occurred before we issued our first NSL report in March 2007, which identified the serious deficiencies in the FBI's use of and oversight of NSLs, and before the FBI began to implement its corrective actions. Therefore, not surprisingly, our follow-up report on the use of NSLs in 2006 contains findings similar to our March 2007 report regarding deficiencies in the FBI's use of NSLs.

Our review of the FBI's use of NSLs in 2006 found a continued upward trend in the use of NSLs, with 49,425 NSL requests issued in 2006, a 4.7 percent increase from the previous year. For the 4-year period 2003–2006, the FBI issued more than 192,000 NSL requests.

National Security Letter Requests (2003 through 2006)



FBI data showed that, on average, approximately one-third of all FBI counterterrorism, counterintelligence, and cyber investigations that were open at any time during 2006 used NSLs. Our review also found that the percentage of NSL requests that related to investigations of U.S. persons (as opposed to non-U.S. persons) continued to increase, rising from about 39 percent of all NSL requests in 2003 to approximately 60 percent of all NSL requests in 2006.

Similar to findings in our first report on the effectiveness of NSLs, our follow-up report found that FBI personnel continued to believe that NSLs were indispensable tools in national security investigations in 2006. They reported that NSLs were used to identify the financial dealing of investigative subjects, confirm the identity of subjects, support the use of enhanced intelligence techniques, and establish predication for the initiation of preliminary and full counterterrorism and counterintelligence investigations.

As required by the Reauthorization Act, our review also examined whether NSLs issued after the effective date of the Reauthorization Act contained the required cer-

tifications to impose non-disclosure and confidentially requirements on NSL recipients. In the random sample of NSLs we reviewed, we found that 97 percent of the NSLs imposed non-disclosure and confidentiality requirements, and almost all contained the required certifications. We found that a small percentage of the justifications for imposing this requirement were perfunctory and conclusory, and a small number of the NSL approval memoranda failed to comply with internal FBI policy.

We also determined that 17 NSL approval memoranda (5 percent of the random sample) contained insufficient explanations to justify imposition of these obligations. We also identified eight NSLs in our sample that contained recitals about non-disclosure that were inconsistent with the corresponding approval memoranda, signifying that case agents, their supervisors, and Chief Division Counsels were not careful in reviewing and approving these documents to ensure consistency. In addition to these non-compliant NSLs that were part of the random sample, we identified eight "blanket" NSLs issued by senior Counterterrorism Division officials in 2006 that did not contain the required certifications.

With regard to intelligence violations arising from the use of NSLs in 2006, our report's findings were consistent with the findings in our first report on NSL usage from 2003 through 2006 and with the results of the FBI's 10 percent review of field office NSLs, which identified at least 640 potential intelligence violations over the 4-year period.

In addition, in our review we determined that FBI personnel self-reported 84 possible intelligence violations involving the use of NSLs in 2006 to FBI Headquarters. Of these 84 possible violations, the FBI concluded that 34 needed to be reported to the President's Intelligence Oversight Board (IOB) in 2006. The 34 matters reported to the IOB included errors such as issuing NSLs without proper authorization, improper requests, and unauthorized collection of telephone or Internet e-mail records. We found that 20 of these violations were attributable to mistakes made by the FBI, while 14 resulted initially from mistakes by recipients of NSLs.

We found that of the 84 possible intelligence violations identified and reported to the FBI Office of the General Counsel in 2006, the FBI received information it was not entitled to receive in 14 matters. In one of the matters the FBI requested information it was not entitled to under the applicable NSL statute. In the other 13 matters, the FBI made proper requests but, due initially to third party errors, obtained information it was not entitled to receive under the pertinent NSL statutes.

We noted that the number of possible NSL-related intelligence violations identified by FBI personnel in 2006 was significantly higher than the number of reported violations in prior years. From 2003 through 2005, the FBI had self-identified only 26 possible intelligence violations, of which 19 were reported to the IOB. We believe that the increase in 2006 may be explained in large part by the attention that our first NSL review, which was ongoing in 2006, focused on these issues and also to increased training, guidance, and oversight by the FBI.

Our follow-up report also noted that a large number of possible intelligence violations were initially attributable to mistakes made by NSL recipients. However, we believe the FBI may have compounded these errors by not recognizing the overproductions and using or uploading the inappropriately obtained information. The FBI Office of the General Counsel is in the process of determining whether the FBI will report these matters to the IOB.

It is important to note that the most serious violations involving the use of NSL authorities in 2006 related to the FBI's use of exigent letters. Our first NSL report generally described this practice by which the FBI improperly obtained telephone toll billing records from three communication service providers pursuant to more than 700 exigent letters without first issuing NSLs. We found that these exigent letters contained inaccurate statements, circumvented the requirements of the Electronic Communications Privacy Act NSL statute, and violated Attorney General Guidelines and internal FBI policy. The OIG is in the process of completing a separate investigation examining the use of exigent letters, as well as the use of "blanket NSLs" and other improper requests for telephone records. Among other things, our upcoming report will assess the accountability of FBI personnel for these practices.

Our NSL report also contains 17 additional recommendations to help improve the FBI's use and oversight of this important intelligence tool. These include recommendations that the FBI provide additional guidance and training for FBI agents on the proper use of NSLs and on the review, filing, and retention of NSL-derived information; reinforce the need for FBI agents and supervisors to determine whether there is adequate justification for imposing non-disclosure and confidentiality requirements on NSL recipients; regularly monitor the preparation and handling of NSLs; and provide timely reports of possible intelligence violations to FBI Headquarters. We also recommended that the Department's working group consider fur-

ther measures for minimizing the retention of NSL-derived information. In its response to our report, the FBI agreed with all of these recommendations and stated that it would implement additional actions to address our findings.

II. SECTION 215 ORDERS

As also required by the Patriot Reauthorization Act, in a second follow-up report issued along with the NSL report the OIG examined the FBI's use of Section 215 orders to obtain business records in 2006. Section 215 of the Patriot Act allows the FBI to seek an order from the FISA Court to obtain "any tangible thing," including books, records, and other items, from any business, organization, or entity, provided the item or items are for an authorized investigation to protect against international terrorism or clandestine intelligence activities. Examples of the types of business records that can be obtained through Section 215 orders include driver's license records, public accommodations records, apartment records, and credit card records.

The OIG's first Section 215 report in March 2007 examined the FBI's use of this authority in calendars years 2002 through 2005. Our recent follow-up report examined the FBI's use of Section 215 authorities in 2006 and, as required by the Patriot Reauthorization Act, also assessed the minimization procedures for business records that the Attorney General was required to adopt in 2006.

Our follow-up review found that, similar to the findings in our first report, the FBI and the Department's Office of Intelligence Policy and Review (OIPR) processed FBI requests submitted to the FISA Court for two different kinds of applications for Section 215 orders in 2006: "pure" Section 215 applications and "combination" Section 215 applications. A "pure" Section 215 application is a term used to refer to a Section 215 application for any tangible item, and it is not associated with any other FISA authority. A "combination" Section 215 application is a term used to refer to a Section 215 request that is added to a FISA application for pen register/trap and trace orders, which identify incoming and outgoing telephone numbers called on a particular line.

In 2006, the FBI and OIPR processed 15 pure Section 215 applications and 32 combination Section 215 applications that were formally submitted to the FISA Court. All 47 applications were approved by the FISA Court. Six additional Section 215 applications were withdrawn by the FBI before they were formally submitted to the FISA Court.

The OIG's follow-up report found that FBI agents encountered similar processing delays for Section 215 applications as those identified in our previous report. Overall, the average processing time for Section 215 orders in 2006 was 147 days, which was similar to the processing time in 2005. However, the FBI and OIPR were able to expedite certain Section 215 requests in 2006, and when the FBI identified two emergency requests the FBI and OIPR processed both requests quickly.

Our follow-up report did not identify any illegal use of Section 215 orders in 2006. However, we identified two instances in 2006 when the FBI received more information than it had requested in the Section 215 orders. In one of the cases, approximately 2 months passed before the FBI recognized it was receiving additional information that was beyond the scope of the FISA Court order. The FBI reported this incident to the IOB, and the additional information was sequestered with the FISA Court.

In the other case, the FBI quickly determined that it had inadvertently received information not authorized by the Section 215 order and isolated the records. However, the FBI subsequently concluded that the matter was not reportable to the IOB and that the FBI should be able to use the material as if it were "voluntarily produced" because the information was not statutorily protected. We disagreed with the FBI's conclusion, and our report recommended that the FBI develop procedures for identifying and handling information that is produced in response to, but outside the scope of, a Section 215 order.

The Reauthorization Act also directed the OIG to identify any "noteworthy facts or circumstances" related to the use of Section 215 orders. Our report discussed another case in which the FISA Court twice refused to authorize a Section 215 order based on concerns that the investigation was based on protected First Amendment activity. The FBI subsequently issued NSLs to obtain information about the subject based on the same factual predicate and without a review to ensure the investigation did not violate the subject's First Amendment rights. We questioned the appropriateness of the FBI's actions because the NSL statute contains the same First Amendment caveat as the Section 215 statute.

As noted throughout the report, the FBI determined that much of the information about this and other cases described in the Section 215 report was classified and therefore had to be redacted from the public report. However, the full classified re-

port contains the details about this case and other cases, and describes other uses of Section 215 authority. The full classified report has been provided to the Department and Congress.

Finally, as directed by the Reauthorization Act, we examined the interim minimization procedures adopted by the Department in 2006 for Section 215 orders. Such procedures are intended to minimize the retention and prohibit the dissemination of non-publicly available information about U.S. persons. We concluded that the interim minimization procedures adopted in September 2006 do not provide specific guidance for minimization procedures that the Reauthorization Act appears to contemplate. Consequently, our report recommends that the Department develop specific minimization procedures relating to Section 215 orders.

III. CONCLUSION

In sum, we believe that the FBI has devoted significant time, energy, and resources to ensuring that its employees understand the seriousness of the FBI's shortcomings with respect to use of national security letters and the FBI's responsibility for correcting these deficiencies. However, the FBI's and the Department's corrective measures are not yet fully implemented, and it is too early to determine whether these measures will eliminate the problems we found with use of these authorities. Ensuring full compliance with the proper use of these authorities will require continual attention, vigilance, and reinforcement by the FBI, the Department, the OIG, and the Congress.

That concludes my prepared statement. I would be pleased to answer any questions.

Mr. NADLER. I thank the gentleman.

Ms. Caproni is recognized for 5 minutes.

TESTIMONY OF VALERIE E. CAPRONI, GENERAL COUNSEL, OFFICE OF THE GENERAL COUNSEL, FEDERAL BUREAU OF INVESTIGATION

Ms. CAPRONI. Good afternoon, Chairman Nadler, Ranking Member Franks and Members of the Committee.

Thank you for inviting me to testify today concerning National Security Letters.

First, let me apologize to Chairman Nadler for the late submission of my written statement. As you know, as a component of the department, my statement has to be cleared by OMB and the Department of Justice before submission, and that took longer than expected. But I will certainly take back to the department your concerns and your objections to the late submission.

The Inspector General has now issued two reports regarding the FBI's use of National Security Letters. Although those reports revealed a number of ways in which the FBI fell short of what is expected, today I would like to address three of his findings.

First, the I.G. found no deliberate or intentional misuse of NSLs, although there were clearly failures of internal controls, as well as instances in which we had inadequate controls and training. The I.G. did not find any evidence of the FBI seeking records without a legitimate investigative purpose.

With the exception of the exigent letter problem that I will come back to, the vast majority of errors involved third party errors, that is, the recipient of the NSL giving us more information than we asked for, or inattention to detail—shortcomings that are not to be excused, but which are far different from intentionally obtaining records that we are not entitled to.

Second, the recent I.G. report provides numerous examples of cases in which NSLs were critical to investigations of individuals who wished to do the United States harm, either through terrorist

acts or counterintelligence activities. FBI personnel told the I.G. that NSLs are critical tools.

Put in the current vernacular, NSLs are needed to connect the dots that the American people and Congress have told us, loudly and clearly, that they expect us to connect.

Finally, the I.G. has acknowledged that the FBI has made substantial strides forward in correcting the lapses previously identified, and we appreciate him acknowledging that. We agree with him that it is too early to know for sure whether these actions will solve everything. But we fervently hope and believe that, with sustained efforts, the controls, policies, procedures and training that we have implemented should eliminate the sorts of errors identified by the Inspector General.

Before I end, I would like to address briefly exigent letters, which was, in my view, the single most troubling discovery by the Inspector General.

As your staffers have been briefed, we are in the process of cleaning up the exigent letter problem, including unraveling the so-called "blanket NSLs" that were mentioned in the I.G.'s recent report. We are looking at every telephone number that appears on a so-called blanket NSL or on an exigent letter that we are aware of. In some instances we have found that appropriate process has previously been issued.

In other instances we have found that, although a number appears on an exigent letter or one of the blanket NSLs, we have no records at all regarding that telephone number. If we have records and no evidence that appropriate legal process has previously been issued for the records, we are evaluating whether the number is relevant to any investigation currently open.

If so, a corrective National Security Letter or grand jury subpoena will be issued. But the phone company will be directed to give us no further records, since we already have the record.

If there is no open investigation because of the passage of time between getting the records and now—and you will recall that the exigent letter problem has been going on for some period of time—at that point, we will evaluate whether, at the time we received the records, there was a true emergency that would have justified disclosure of those records without legal process under 18 U.S.C. 2702. If so, the emergency that existed at that time is documented, and the records are retained.

One example of such a situation would be the emergency that existed, and the phone records that we retained, in the immediate wake of the disrupted plot to blow up jetliners as they flew over the Atlantic Ocean.

If there is no currently open investigation, and there was no emergency at the time we received the records, the records are removed from our files and destroyed. This has been a laborious, time-consuming process.

And I can assure this Committee that our efforts have been designed to ensure that the FBI does not retain any record that it should not have, while maintaining those records that could be a dot that needs to be connected, in order to keep the country safe.

In conclusion, the FBI believes that National Security Letters are important tools in our national security arsenal, and we are committed to using them effectively and legally.

I am happy to answer any questions the Committee may have.

[The prepared statement of Ms. Caproni follows:]

PREPARED STATEMENT OF VALERIE E. CAPRONI

Statement of
Valerie E. Caproni
General Counsel
Federal Bureau of Investigation
Before the
Committee on the Judiciary
United States House of Representatives
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
Concerning
National Security Letters
April 15, 2008

Good afternoon Mr. Chairman, Ranking Member Franks, and Members of the Subcommittee. It is my pleasure to appear before you today to discuss with the Subcommittee the FBI's use of national security letters (NSLs), particularly in light of the Inspector General's report released on March 9, 2007, and his follow-on report released on March 13, 2008. The IG's reports are fair, acknowledging the importance of NSLs to the ability of the FBI to conduct the national security investigations that are essential to keeping the country safe. Importantly, the Office of the Inspector General (OIG) found no deliberate or intentional misuse of the NSL authorities, Attorney General Guidelines, nor FBI policy. Furthermore, I want to emphasize two extremely important points regarding the IG's second report (i.e., the one released on March 13, 2008). That report covered 2006, before the FBI had in place its modifications designed to ensure the NSL problems the IG identified in his initial report are not repeated. As a result, the problems addressed in the second report obviously do not reflect a failure to respond to the 2007 IG report. Second, we appreciate that the IG in his second report found that we have made

tremendous strides in resolving the problems previously identified and that we appear to be on track to implementing policies and procedures to minimize the likelihood that the problems will recur. Specifically, the IG found that the FBI has made significant progress responding to the issues raised in the first report and that the FBI's leadership has made this issue a top priority.

Although not intentionally, we fell short in our obligation to report to Congress on the frequency with which we use this tool and in establishing rigorous internal controls to ensure all NSLs were served strictly in accordance with legal requirements and to ensure that any materials received from third parties were in strict compliance with the NSL served on that party. Director Mueller concluded from the IG's 2007 report that we need to redouble our efforts to ensure that there would be no repetition of the mistakes of the past, however lacking in willfulness, and I share his commitment. We appreciate the attention of Congress to these audits, which were called for in the USA PATRIOT Improvement and Reauthorization Act. We welcomed the OIG's reviews regarding this important tool's use. The first report made 10 recommendations and the second made 17 recommendations. The recommendations were designed to provide controls over the issuance of NSLs, the creation and maintenance of accurate records necessary for Congressional reporting and procedures to ensure that "over productions" (i.e., records from NSL recipients that were not called for by the NSL) were appropriately handled. The FBI fully supports each of the 27 recommendations and concurs with the IG that, when implemented, these reforms will ensure full compliance with both the letter and the spirit of the authorities entrusted to the Bureau.

H.R. 3189

We are aware of H.R. 3189, currently titled as the proposed National Security Letters Reform Act of 2007, that was introduced last July and subsequently referred to this Subcommittee last September. Important to the consideration of any legislative changes are the many oversight and internal control mechanisms that the FBI has established since the release of

the IG's first report. We believe these are important steps and that, in light of the FBI's tremendous progress in this regard, further legislative changes, including the measures envisioned by H.R. 3189, would be neither necessary nor appropriate.

FBI Corrective Measures

Several years ago, the FBI's process for tracking NSLs for Congressional reporting purposes shifted from a totally manual process, where NSL data were written on 3 x 5 cards, to a standalone Access database. This database is referenced in the first IG report as the OGC database. While the OGC database was a giant technological step forward from 3 x 5 cards, it was not an adequate system given the increase in NSL usage since 9/11. Approximately two years ago, we recognized that our technology was inadequate, and we began developing a system for improved data collection. The new system, in addition to improving data collection, now automatically prevents many of the NSL-related errors referenced in the IG reports. Specifically, we built an NSL subsystem within the already existing, highly successful FISA Management System (FISAMS) to function as a workflow tool that automates much of the work in preparing NSLs and their associated paperwork. The NSL subsystem is designed to require the user to enter certain data before the workflow can proceed and requires specific reviews and approvals before the request for the NSL can proceed. Through this process, the FBI can automatically ensure that certain legal and administrative requirements are met and that required reporting data is accurately collected. For example, by requiring the user to identify the investigative file from which the NSL is to be issued, the system verifies the status of that file to ensure that it is still open and current, and it ensures that NSLs are not being requested out of control or administrative files. The system requires the user to identify separately the target of the investigative file and the person about whom records are being obtained through the requested NSL, if different. This allows the FBI to count accurately the number of different persons about whom we gather data through NSLs. The system also requires that specific data elements be

entered before the process can continue, such as requiring that the target's status as a U.S. Person (USPER) or non-USPER be entered. The system does not permit requests containing logically inconsistent answers to proceed.

The NSL subsystem was designed so that the FBI employee requesting an NSL enters data only once. Among other things, this minimizes transcription errors that give rise to unauthorized collections that must be reported to the Intelligence Oversight Board (IOB). In addition, requesters are required to provide the narrative necessary to explain why the NSL is being sought, the factual basis for making a determination that the information is relevant to an appropriately predicated national security investigation, and the basis for a determination that the NSL should include a non-disclosure provision, if such a provision is included within that particular NSL. As with the FISA Management System, this subsystem has a comprehensive reporting capability.

We began working with developers on the NSL subsystem in February 2006, and after a brief piloting period, its rollout was completed on January 1, 2008. Now, as we move forward, and as we continue to make minor system modifications to address certain situations, I am more confident that the data we report to Congress on NSLs issued subsequent to January 1, 2008 will be as accurate as possible.

One particularly significant finding in the IG's first report involved the use within one unit at Headquarters of so-called "exigent letters." These letters were provided to telephone companies with requests for toll billing information regarding telephone numbers. All of the letters stated that there were exigent circumstances. Many of the letters stated that federal grand jury subpoenas had been requested for the records even though, in fact, no such request for grand jury subpoenas had been made, while others promised national security letters. From an audit and internal control perspective, the FBI did not document the nature of the emergency circumstances that led it to ask for toll records in advance of proper legal process, did not keep

copies of the exigent letters it provided to the telephone companies, and did not keep records showing whether it had subsequently provided either the legal process promised or any other legal process. Further, based on interviews the IG conducted, some employees indicated that there was not always any emergency relating to the documents that were sought.

The FBI is working jointly with the IG in its investigation of the exigent letter situation. Because that matter is still under investigation, I cannot address it in any depth. However, I would like to emphasize that, in response to the obvious internal-control lapses this situation highlights, changes have already been made to ensure that this situation does not recur. Now, any agent who needs to obtain records protected under the Electronic Communications Privacy Act (ECPA) on an emergency basis must do so pursuant to 18 U.S.C. § 2702. Section 2702(c)(4) permits a carrier to provide non-content information regarding its customers to the government "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency[.]" Although not required by the statute, FBI policy requires that a request for such disclosure generally must be in writing and must clearly state that the disclosure without legal process is at the provider's option. The request for documents must be approved at a level not lower than Assistant Special Agent in Charge (ASAC) in a field office and not lower than Section Chief at Headquarters. The letter request must set out the basic facts of the emergency so that the provider can make some assessment whether it concurs that there is an emergency. In addition, the fact that documents were obtained pursuant to a 2702 letter as well as ASAC approval must be documented in an Electronic Communication (EC). While the policy allows for oral approval by the ASAC, OGC requires that the approval be documented after the fact if it is not possible to do so prior to receipt of the records. We believe this policy permits our agents to obtain quickly telephone records in cases of true emergency while creating strong internal control mechanisms, which are subject to audit, to ensure that 2702 is not abused.

One important realization--across the board, not merely in the context of NSLs--was that, although the FBI generally had appropriate procedures in place, it did not have an effective mechanism to ensure that the procedures were being followed. As a result, the Director established a new Office of Integrity and Compliance, reporting to the Deputy Director, to identify proactively those areas where there are weaknesses or potential weaknesses in internal controls, inadequate policies or training, or inadequate compliance mechanisms and to address them. As the Director recently testified before another House Subcommittee: "The lesson we learned from this episode is that it's insufficient to issue procedures without also having a mechanism to assure that the procedures are being followed in our 56 field offices and in our 400 resident agencies."

Other corrective measures the FBI has implemented include, for example, a very important and comprehensive EC, dated June 1, 2007, that set forth in one document all FBI policy regarding NSLs. The preparation of that EC involved, among other things, meetings with various national-level privacy groups and certain congressional staff members. Extremely valuable suggestions resulted from those meetings, many of which were incorporated into the FBI's guidance. The EC and other FBI guidance now require, for example, that all NSLs must be reviewed and approved by a Chief Division Counsel, an Associate Division Counsel, or an attorney within the FBI's National Security Law Branch. These attorneys must provide independent legal review of all NSLs. The guidance also bars the use of exigent letters, requires reviewers to ensure relevance to an open national security investigation and compliance with other statutory and procedural requirements, outlines how so-called "over-collected material" must be handled, and requires signed copies of the NSLs to be retained. Furthermore, to implement these policy changes and to educate FBI employees on common NSL-related problems, we have placed heavy emphasis on NSLs in our training of agents, analysts, and other employees involved in national security investigations. Now, whenever an attorney from the

National Security Law Branch visits a field office, that attorney conducts training on NSLs. In addition, we created a detailed online NSL training course which is required for every employee who is involved in drafting, reviewing, or approving NSLs.

Conclusion

We in the FBI know that we can accomplish our mission of keeping the country safe only if we are trusted by all segments of the American public. With events like the London terror attacks of 3 years ago and the Canadian plot to use fertilizer bombs to destroy buildings in Canada in 2006, we have all been reminded of the risk of a catastrophic attack from homegrown terrorists. Our single best defense against such an attack is the eyes and ears of all Americans--but particularly of those segments of the population in which the risk of radicalization is the highest. We need people in those communities to call us when they hear or see something that looks amiss. We know that we reduce the probability of that call immeasurably if we lose the confidence of those segments of the population. It is for that reason that we continually look for ways to assure all Americans that we respect their individual rights, including privacy rights, and that we use the tools that have been provided to us consistent with the rules set by Congress.

I appreciate the opportunity to appear before the Subcommittee, and look forward to your questions. Thank you.

Mr. NADLER. I thank the witnesses, and we will now have a round of questioning for the witnesses.

I will grant myself 5 minutes for questioning.

I will start with Ms. Caproni.

Ms. Caproni, you testified that the FBI has done a sufficient job of self-reporting and does not need any statutory remedies to address the abuses uncovered by the I.G.'s report. Just today, however, the Electronic Frontier Foundation disclosed that documents obtained by the EFF to a Freedom of Information Act request show that a misuse of the FBI's National Security Letter authority—issued at the direction of FBI headquarters, not a field office—went unreported to the Intelligence Oversight Board for almost 2 years.

Given that, and the numerous reports of abuse, how is Congress and the public supposed to trust that the department is capable of self-policing? Don't we need to restore the trust in our intelligence community and checks on our process? And why didn't anyone formally report this matter to the OIG until February of last year?

Ms. CAPRONI. The incident that you are referring to that was reflected in documents that the EFF recently released was, first off, well before the reforms that we put into place subsequent to the I.G.'s March 2007 report.

Mr. NADLER. Subsequent to what? I am sorry?

Ms. CAPRONI. The events occurred prior to the actions that we have taken following the I.G.'s earlier report. That is, we have put into place a number of controls now, that I believe would have first resulted in that NSL not being issued. Or second, if it was issued, being reported much more promptly.

In terms of why there was such a delay between the time that there was public knowledge of that NSL—and there was public knowledge, because it was reported in the press—and March of 2007, is unclear to me. There was a direction made to report the incident. It did not get reported. When we discovered it had not been reported, it was directed to be reported, and it then was reported.

Mr. NADLER. Thank you.

Now, both you and the Inspector General have expressed the lack of intentional misuse of the NSL authority, all due to improper—I should not say "improper"—insufficient training, and so forth. But the "Washington Post" has reported that there was at least one IOB report of willful and intentional misconduct.

Does the FBI consider the use of an NSL to seek records beyond the scope of this statute at the specific direction of FBI headquarters not deliberate or intentional?

Ms. CAPRONI. Chairman Nadler, again, I am not quite sure why the direction was given to issue an NSL in that case. As I look at what I believe they were seeking from the university, an NSL was not the appropriate way to go.

It was unclear to me whether this was simply a miscommunication. I find it hard to believe that the intent, since we were entitled to the records, and we obtained the records, pursuant to a grand jury subpoena, with the approval of a court.

This was not an issue of we were seeking records that we were not entitled to. An NSL was the wrong tool to use.

So it is unclear to me why headquarters directed that an NSL be used.

Again, I think my—what I am stressing is, there is no evidence of the Bureau using these NSLs to get documents——

Mr. NADLER. That they were not——

Ms. CAPRONI. They were simply irrelevant to our investigative mission.

Mr. NADLER. Now, you stated that the majority of abuses were made by third parties, not by the FBI.

Now, when a third party gives you too much improper information, what do you do with it? Can you look at it and issue another NSL to get that very information or more? And wouldn't that be along the line of using evidence that is the fruit of the poisonous tree?

Ms. CAPRONI. Let me address both issues.

First let me say that we now have in place policies and procedures that require the case agents to review the returns to make sure there is no overproduction. They cannot know whether they have got an overproduction unless they actually look at what they received.

If they have received information that is in excess of what the NSL has called for, they have to sequester the information.

They can then make a decision. If what has happened is the provider has provided us 2 extra weeks of bank records—so those records are still relevant to the investigation, it would be unusual that they would not be relevant—they can issue a new NSL for that additional information.

If it is totally irrelevant—that is, maybe they inadvertently provided us the wrong customer—that information is not relevant to the investigation, so it cannot be used in any way, nor can they issue another NSL for it. That will be sequestered, and eventually be returned to the provider or destroyed.

Mr. NADLER. Okay.

Ms. CAPRONI. More generally, though, your question about fruit of the poisonous tree, I would like to address.

Fruit of the poisonous tree is a constitutional doctrine that derives from a constitutional violation. It is important to stress that these are not constitutional violations.

These are third party records held by third parties. There is no violation of the customer's fourth amendment rights. When we obtain the records that may be in excess of——

Mr. NADLER. But wait a minute. If the third party violated, you could very well have a violation of the customer's fourth amendment rights.

Ms. CAPRONI. With all due respect, sir, that would not be correct under current Supreme Court precedents.

Mr. NADLER. Because it is not the government doing it directly.

Ms. CAPRONI. No. It is because the records—the customer, the customer's privacy interests in the records is not constitutionally protected. Under existing Supreme Court precedent, once they share the information with a third party, the third party is free to disclose that information.

Mr. NADLER. And doesn't that argue that, in order to protect those privacy records, there have got to be some checks on the third party?

Ms. CAPRONI. There are checks on the third party. Congress has passed a number of different privacy statutes that provide statutory protection for the documents.

Mr. NADLER. And given the fact that everything here is secret, how are those protections guaranteed or enforced?

Ms. CAPRONI. The issue of the secrecy versus the protection are kind of two separate things.

Mr. NADLER. Well, but they interact with each other.

Ms. CAPRONI. The provider is still subject to a statutory requirement that they not release the records without appropriate process. That is their obligation.

Whether they comply, or even if they violate the statute, there is not a constitutional violation. There is a statutory violation.

Mr. NADLER. My time has expired, and I recognize the gentleman from Arizona for 5 minutes.

Mr. FRANKS. Well, Mr. Chairman, thank you.

Ms. Caproni, you have testified that National Security Letters generally permit us to obtain the same sort of documents from third party businesses and prosecutors that agents obtain in criminal investigations with grand jury subpoenas, essentially all the time. But these are, of course, domestic criminal investigations.

NSLs have been instrumental in breaking up cells like the Lackawanna Six and the Northern Virginia Jihad. Through the use of NSLs, the FBI has traced sources of terrorist funding, established telephone linkages that resulted in further investigations and arrests, and allow the FBI to link terrorists together financially and pinpoint cells and operatives by following the money.

In other words, it gives us some dots to connect. It is not just a line. We do not just get a few triangles. We get a picture that helps us solve or prevent some of these very serious potential acts of terrorism against Americans.

Can you elaborate on what the loss of such a tool would be? And perhaps even answer first, are we somehow thwarting the constitutional rights of American citizens here?

Ms. CAPRONI. Again, absolutely not. These are records that are being held by third parties. There is not a fourth amendment constitutional protection for those vis-a-vis the customer of the record.

In terms of the importance of National Security Letters, they are critically important to our ability to do our job. By getting records with National Security Letters, things like phone records and bank records, those are the basic building blocks of any investigations.

In a criminal investigation, they are critical. They are there, kind of grand jury subpoenas, or, depending on the type of case, with an administrative subpoena.

In the national security context, when we are looking at terrorists, or intelligence officers for spies, where the risk to the country is much higher, we use National Security Letters to get the documents.

But the same underlying need exists, which is to build enough information about the person, about the subject of our investigation, to know whether or not this is someone who intends to do us

harm, and therefore, we need to follow them, figure out who their compatriots are, so that we can disrupt and dismantle their organization, or whether in fact they intend no harm, in which case we close the investigation and move on.

Without the ability to get these sorts of records, we will be stopped in our tracks before we ever begin.

Mr. FRANKS. Well, you know, many FBI personnel have told us that the NSLs are an essential and indispensable intelligence tool.

And I guess, Ms. Caproni, I do not want to put words in your mouth. I mean, from my perspective, this seems that through the use of these NSLs, that we are doing everything that we can to get at terrorists, while at the same time doing everything we possibly can to observe the constitutional rights of anyone in America, whether they be citizen or otherwise, that the effort here is to truly protect American citizens and to defend ourselves in a preventative capacity from being attacked in this country.

So, I will just ask a couple of basic questions, put it in your words. Do you think, once again, that we are thwarting the Constitution here, that somehow we are subjecting people on American soil to unconstitutional search and seizure, or somehow thwarting their civil rights?

Ms. CAPRONI. Absolutely not.

Mr. FRANKS. And yet you are saying to me that this is a vital tool in being able to help prevent—identify, prevent and defend this country against terrorism?

Ms. CAPRONI. Absolutely. I do not believe that we could do the job that Congress and the American people expect us to do, in terms of keeping us safe from terrorism and from spies and those who would steal our secrets, without National Security Letters.

Mr. FRANKS. Well, Ms. Caproni, I could probably elaborate, but I just wish that those basic points could be put forward. Because sometimes there is a lot of noise that goes around here and a lot of political grandstanding. But the reality is here that the desire of this country is to protect its citizens, to protect their constitutional rights. And unfortunately, terrorists have other ideas, and they have to be dealt with in ways that we really have little alternative.

It is about an intelligence gain. If we knew where every terrorist was in the world today and what they were up to, the war on terror would be over in 2 months. But unfortunately, we do not.

So, I just thank you for your service to the country and for doing everything you can to protect the citizens of this country.

Mr. NADLER. I thank the gentleman.

I now recognize the gentleman from Virginia for 5 minutes.

Mr. SCOTT. Thank you.

Ms. Caproni, I am sure some of the letters are necessary. Are all of these NSLs necessary?

Ms. CAPRONI. I am sorry. Are all of these——

Mr. SCOTT. Are all of them absolutely necessary for the protection of the national security?

Ms. CAPRONI. Well, I believe they are. I do not think agents issue National Security Letters to get records that are not relevant to their investigations and needed, in order either to close out a lead, you know, to—for us to ascertain that the person does not pose a

risk to the country, or, in fact, to disclose that the person does pose a risk.

Mr. SCOTT. Now, exactly where is the oversight in all of this?

Ms. CAPRONI. The oversight comes in a number of different ways. First off, there are congressionally mandated juries. And the Inspector General's reports obviously provided a great deal of oversight.

Subsequent to the March 2007 report, we have mandated that there are—there must be legal review of any NSL before it is issued. I think that is one——

Mr. SCOTT. Say that again?

Ms. CAPRONI. Subsequent to the March 2007 Inspector General's report, as a matter of internal policy, the FBI has mandated that there must be legal review of any NSL before it is issued.

Mr. SCOTT. And so, the check and balance is within the same agency that is doing the issuing of the NSL?

See, some of us think check and balance means you check with another branch of government. And we have another concept of check and balance. You check with your co-workers. And if your co-worker says what you are doing is okay, then it is okay. That is not what some of us thought really was a check and balance.

Ms. CAPRONI. If I could just continue on the other controls.

And might I also say that I think the lawyers in the Bureau, many of whom work directly for me, take their responsibility relative to reviewing National Security Letters very seriously. And if the material that is laid out in the document supporting the NSL does not support the issuance of an NSL, the lawyer will not sign off on it.

Mr. SCOTT. And these are all people who are hired by the same attorney general. I mean, it is all within the same agency.

Ms. CAPRONI. That is correct.

Mr. SCOTT. So, when that person says, this is what I want, all of his employees are checking and balancing themselves.

Ms. CAPRONI. Again, the director of the FBI has made it very clear that he wants to achieve the mission of the FBI, but to achieve it lawfully. So, the mission of the employees of the FBI is to achieve these goals consistent with the law.

Mr. SCOTT. But what happens if they—what happens if he decides that he wants to do a little political shenanigan? What happens then? What are the checks and balances?

Ms. CAPRONI. There is absolutely no evidence that this director of the FBI would ever engage in political shenanigans.

Mr. SCOTT. Okay. Well, you know, the attorney——

Ms. CAPRONI. If I could get to the third——

Mr. SCOTT. Well, let me just say this. As part of—when I listen to this, we are also listening and trying to get an answer out of the Department of Justice as to whether or not U.S. attorneys were fired because they did not indict Democrats in time affect the next election. And so, we have not had a credible response to that.

So, sometimes we suspect that there may be some political shenanigans going on. And we are just asking where the checks and balances are.

Ms. CAPRONI. Well again, I would say, Mr. Fine works for the Department of Justice, too. And it seems to me he has provided

very vigorous oversight. So I think, merely because your paycheck comes from the Department of Justice does not mean that you are not capable or desirous of obeying the law and providing the appropriate legal advice to your client.

Mr. SCOTT. Under the——

Ms. CAPRONI. If I could just—I cannot answer for the Department of Justice in why they are not providing the documents. That is not within the scope of my responsibilities.

But the third element of oversight that I think is important for this Committee to recognize is, again, subsequent to the March 2007 report and subsequent to Congress establishing the National Security Division within the Department of Justice, the National Security Division has set up an oversight within the National Security Division.

Those attorneys go out to field offices and do what are called national security reviews. They have access to everything in the file. They can go through it from soup to nuts.

Mr. SCOTT. And this is the same agency, though. They are employed by the same agency.

Ms. CAPRONI. Well, they are Department of Justice attorneys.

Mr. SCOTT. Okay.

What happened with this—what did the Supreme Court decide in—decided it was unconstitutional in September 6, 2007?

Ms. CAPRONI. I am sorry. Say again?

Mr. SCOTT. Excuse me. The district court in 2007, what did the court strike down, and what is the status of those——

Ms. CAPRONI. Is that the Southern District case?

Mr. SCOTT. Yes.

Ms. CAPRONI. I do not know the date——

Mr. SCOTT. Southern District of New York, yes.

Ms. CAPRONI. That case is pending on appeal. I believe it has been fully briefed in the Second Circuit, but it might not quite be fully briefed. So I would anticipate argument in the next few months.

That case did, as Chairman Nadler pointed out, hold that there was, even after the PATRIOT Act Reauthorization Act, which changed the rules on disclosure and nondisclosure of National Security Letters by the recipient, Judge Marrero found, nonetheless, that the new statute continues to be unconstitutional under the first amendment. That is what is pending on appeal, is whether, in fact, the structures that the Congress passed in the PATRIOT Reauthorization Act was constitutional under the first amendment.

There is also an issue about whether the gag provisions of that bill are severable. That is, would Congress prefer there to be no national security statute, that there is not a requirement, or can we sever the requirement as being unconstitutional and keep the balance of the statute?

Those are the two primary issues that are pending on appeal before the Second Circuit.

Mr. NADLER. The gentleman's time has expired.

I believe the court, the lower court has decided it was not severable. Correct?

Ms. CAPRONI. That is correct.

Mr. NADLER. Thank you.

We thank the witnesses from the first panel.

We ask that the members of the second panel come forward and take their seats.

And while they are taking their seats, let me perform the introductions.

Jameel Jaffer is the director of the American Civil Liberties Union's National Security Project. The project litigates civil liberties and human rights cases related to detention, torture, surveillance, censorship and secrecy. Mr. Jaffer's own litigation docket includes *Doe v. Mukasey*, a challenge to the FBI's National Security Letter authority.

Before joining the staff of the ACLU, Mr. Jaffer served as law clerk to the Honorable Amelia First, U.S. Court of Appeals to the Second Circuit, and then to the Right Honorable Beverly McLaughlin, Chief Justice of Canada. He is a graduate of Williams College, Cambridge University, and Harvard Law School.

Bruce Fein needs no introduction, but I will introduce him anyway. He is a graduate of Harvard Law School. He joined the U.S. Department of Justice, where he served as assistant director of the Office of Legal Policy, legal adviser to the assistant attorney general for antitrust, and the associate deputy attorney general.

Mr. Fein then was appointed general counsel of the Federal Communications Commission, followed by an appointment as research director for the Joint Congressional Committee on Covert Arms Sales to Iran.

Mr. Fein is an adjunct scholar with the American Enterprise Institute, a resident scholar at the Heritage Foundation, a lecturer at the Brookings Institution and an adjutant professor at George Washington University.

Michael J. Woods served as chief of the FBI's National Security Law Unit from 1997 to 2002, as counsel to the National Counterintelligence Executive in 2002, and as a Department of Justice prosecutor from 1993 to 1997.

During his time at the FBI, Mr. Woods and the lawyers under his supervision were responsible for providing legal advice to agents and analysts involved in counterintelligence and counterterrorism operations, and for the production and review of National Security Letters. Mr. Woods is a graduate of Harvard Law School and of Oxford University.

David Kris is a graduate of Haverford College and Harvard Law School. He clerked for Judge Stephen Trott of the Ninth Circuit, joined the Department of Justice through its honors program. He worked as a prosecutor for 8 years from 1992 to 2000, conducting several trials and arguing appeals across the country.

From 2000 to 2003, he was associate deputy attorney general. In that role, his unclassified responsibilities included supervising the government's use of the Foreign Intelligence Surveillance Act, or FISA, which has been somewhat in the news lately, representing the Justice Department to the National Security Council and in other interagency settings, briefing and testifying before Congress and assisting the attorney general in conducting oversight of the U.S. intelligence community. He is an adjunct professor at Georgetown University Law Center.

Without objection, your written statements will be made part of the record in their entirety. We would ask each of you to summarize your testimony in 5 minutes or less.

As a reminder, there is a timing light at your table. When 1 minute remains, the light will switch from green to yellow, and then to red when the 5 minutes are up.

Before we begin, it is customary for the Committee to swear in its witnesses.

If you would please stand and raise your right hand to take the oath.

Do you swear or affirm under penalty of perjury that the testimony you are about to give is true and correct to the best of your knowledge, information and belief?

Thank you.

Let the record reflect that the witnesses answered in the affirmative.

You may be seated.

We will now call upon the first witness for 5 minutes.

Mr. Jaffer?

TESTIMONY OF JAMEEL JAFFER, DIRECTOR, AMERICAN CIVIL LIBERTIES UNION'S NATIONAL SECURITY PROJECT

Mr. JAFFER. Chairman Nadler, Ranking Member Franks, thank you for inviting me to testify today about National Security Letters and H.R. 3189, the National Security Letter Reform Act.

The NSL statutes invest the FBI with sweeping power to collect information about innocent people, and they allow the agency to impose unconstitutional gag orders on NSL recipients.

Mr. Nadler's bill would introduce much needed safeguards for civil liberties, while preserving the executive's ability to collect information about people who actually pose threats.

I want to highlight two serious problems with the NSL statutes: their impact on wholly innocent people and their authorization of unconstitutional gag orders.

The statutes permit the government to obtain records about people who are not known, or even suspected, to have done anything wrong. Because of changes made by the PATRIOT Act, the FBI can compile vast dossiers about innocent people—dossiers that could include financial information, credit information and even information that is protected by the first amendment.

The Inspector General's audits confirm that the FBI is collecting information about people two and three times removed from actual suspects. Roughly 50,000 NSLs are being issued every year—most seeking information about U.S. persons.

The FBI stresses that NSLs are used only to collect transactional or non-content information. But NSLs reach information that is extremely sensitive.

The FBI can compel an Internet service provider to disclose the identities of people who have visited a particular Web site, a list of e-mail addresses with which a particular person has corresponded, or even the identity of a person who has posted anonymous speech on a political Web site.

Privacy concerns aside, Congress must ask whether it serves national security to create vast databases of information about inno-

cent people. Post-9/11 investigations found that over-collection can divert resources away from the most important investigations and bury the most important information.

Mr. Nadler's bill will protect the privacy of innocent people, while at the same time refocusing the government's antiterrorism resources on actual terror.

Mr. Nadler's bill will also address a second problem with the NSL statutes. The problem is that each of the NSL statutes allows the government to impose gag orders on NSL recipients. These gag orders are not subject to prior judicial review; the FBI imposes them unilaterally.

NSL recipients can challenge the gag orders in court, but the judicial review is toothless. It is the FBI that decides whether secrecy is necessary, and the courts are required to defer to the FBI's decision.

Now, obviously, secrecy is necessary in some national security investigations. But the FBI's power to impose gag orders should be subject to meaningful judicial review. Without that review, the power is easily abused.

The ACLU currently represents someone—I will call him John Doe—who was served with an NSL. Doe believes that the NSL was illegal, but a gag order bars him from explaining why he holds that opinion, or even from disclosing his own identity. For 4 years now, Mr. Doe has been prohibited from telling the public why he believes the FBI is abusing its power. And the FBI continues to enforce the gag order today, even though it abandoned its demand for records more than a year ago.

The Chairman's bill would prevent this sort of abuse.

This past September, a Federal court struck down one of the NSL's statutes in its entirety. The court held that gag orders must be subject to prompt judicial review, and the courts must be permitted to invalidate gag orders that are not narrowly tailored to a compelling government interest. As long as the NSL statutes foreclose a sign of judicial review, the statutes are unconstitutional, and the government risks losing the NSL authority altogether.

Mr. Nadler's bill will align the NSL statutes with the first amendment. Gag orders will not be barred under the bill when secrecy is truly necessary, but rather, they will be limited to those circumstances. Moreover, the bill will ensure that gag orders are no broader than absolutely necessary.

Absent an actual need for secrecy, an Internet service provider should be able to tell the public if it receives an NSL that seeks information about thousands of people. And absent an actual need for secrecy, a library should be able to tell the public if it receives an NSL that seeks information about first amendment activities.

Mr. Nadler's bill would protect first amendment rights, while at the same time allowing for secrecy where legitimate national security concerns compel it. The ACLU commends Mr. Nadler for introducing the bill.

Thank you again for the opportunity to appear today.

[The prepared statement of Mr. Jaffer follows:]

PREPARED STATEMENT OF JAMEL JAFFER

Testimony of Jameel Jaffer
Director of the National Security Project of the
American Civil Liberties Union Foundation

Before
The House Subcommittee on the Constitution,
Civil Rights, and Civil Liberties

Oversight Hearing on
H.R. 3189, the National Security Letters Reform Act of 2007

April 15, 2008

Thank you for inviting me to testify before the Subcommittee on behalf of the American Civil Liberties Union (ACLU), its hundreds of thousands of members, and its fifty-three affiliates nationwide.

We appreciate the opportunity to provide our views about national security letters (NSLs) and about H.R. 3189, the National Security Letters Reform Act of 2007. Because of changes made by the Patriot Act, the NSL statutes allow the FBI to compile vast dossiers about innocent people – dossiers that can include financial information, credit information, and even information that is protected by the First Amendment. The FBI collects this information in complete secrecy. The ACLU feared that the expanded NSL powers would be abused, and recent audits by the Justice Department's Office of Inspector General (OIG) have shown our fears to be well-founded. We believe that H.R. 3189 would provide needed safeguards for civil liberties while preserving government's ability to collect information about individuals who actually pose threats.

My name is Jameel Jaffer and I am the Director of the ACLU's National Security Project. The Project litigates civil liberties and human rights cases relating to detention, torture, surveillance, censorship, and secrecy. Over the past six years, I and my colleagues have brought a number of lawsuits to expose and challenge unlawful government surveillance. Among these lawsuits are several that relate to NSLs. In *Library Connection v. Gonzales*, we represented four Connecticut librarians in a

successful challenge to an NSL served on their organization in 2005.[1] Since 2004, we have also represented an Internet service provider in a facial challenge to the statute that allows the FBI to serve NSLs on "electronic communication service providers." That litigation, now captioned *Doe. v. Mukasey*, resulted in a 2004 decision that found the statute unconstitutional under the First and Fourth Amendments, and ultimately led to the legislative amendments that Congress enacted in 2006.[2] Since Congress acted, we have returned to court to challenge the amended statute, this time focusing solely on the statute's gag provisions. Last year the district court found the amended gag provisions unconstitutional,[3] and the government's appeal is now pending before the United States Court of Appeals for the Second Circuit.

Over the past six years, the ACLU has also brought a number of Freedom of Information Act suits to obtain information about the government's use of NSLs. For example, in 2002 and 2003, we litigated two requests for records about the FBI's issuance of NSLs after the passage of the Patriot Act.[4] Those suits resulted in the first release of information about the FBI's use of NSLs.[5] More recently, we litigated a request for records concerning the issuance of NSLs by the Central Intelligence Agency and Department of Defense; some of the information we obtained through that litigation was made public last week.[6] We are about to file a new lawsuit seeking records about the FBI's issuance of NSLs at the behest of other executive agencies, a practice that allows those agencies to circumvent statutory limitations on their own authority to issue NSLs.

The ACLU has a number of serious concerns with the NSL statutes as they exist now. In this testimony, I focus on only two. The first is that the NSL statutes allow executive agencies (usually the FBI) to obtain records about people who are not known – or even suspected – to have done anything wrong. They allow the government to collect information, sometimes very sensitive information, not just about suspected terrorists and spies but about innocent people as well. The second concern is that the NSL statutes allow government agencies (again, usually the FBI) to prohibit NSL recipients from disclosing that the government sought or obtained information from them. This authority to impose non-disclosure orders – gag orders – is not subject to meaningful judicial

---

[1] 386 F.Supp.2d 66 (D. Conn. 2005), *appeal dismissed as moot*, 449 F.3d 415 (2d. Cir. 2006).

[2] *Doe v. Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004), *vacated as moot sub nom. Doe v. Gonzales*, 449 F.3d 415 (2d. Cir. 2006); USA Patriot Act Improvement and Reauthorization Act of 2005, Pub. L. 109-177, 120 Stat. 195 (Mar. 9, 2006) ("PIRA"); USA Patriot Act Additional Reauthorizing Amendments Act of 2006, Pub. L. 109-178, 120 Stat. 278 (Mar. 9, 2006) ("ARAA").

[3] *See Doe v. Gonzales*, 500 F.Supp.2d 379 (S.D.N.Y. 2007).

[4] *See ACLU v. Dep't of Justice*, 321 F.Supp.2d 24 (D.D.C. 2004); *ACLU v. Dep't of Justice*, 265 F.Supp.2d 20 (D.D.C. 2003).

[5] Some of the records that were made public are available at www.aclu.org/patriotfoia.

[6] Some of the records that were made public are available at http://www.aclu.org/safefree/nationalsecurityletters/32088res20071014.html.

review. Indeed, as discussed below, the review contemplated by the NSL statutes is no more than cosmetic.[7]

I. The NSL statutes invest the FBI with broad authority to collect constitutionally protected information pertaining to innocent people.

Several different statutes give executive agencies the power to issue NSLs. Under 12 U.S.C. § 3414(a)(5)(A), the FBI is authorized to compel "financial institutions" to disclose customer financial records.[8] The phrase "financial institutions" is defined very broadly, and encompasses banks, credit unions, thrift institutions, investment banks, pawnbrokers, travel agencies, real estate companies, and casinos.[9] Under 15 U.S.C. § 1681u, the FBI is authorized to compel consumer reporting agencies to disclose "the names and addresses of all financial institutions . . . at which a consumer maintains or has maintained an account," as well as "identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment." Under 15 U.S.C. § 1681v, executive agencies authorized to conduct intelligence or counterintelligence investigations can compel consumer reporting agencies to disclose "a consumer report of a consumer and all other information in a consumer's file."[10]

---

[7] The ACLU has a number of other concerns with the NSL statutes. First, the statutes do not significantly limit the retention and dissemination of NSL-derived information. *See, e.g.*, 18 U.S.C. § 2709(d) (delegating to the Attorney General the task of determining when, and for what purposes, NSL-derived information can be disseminated). Second, the statutes provide that courts that hear challenges to gag orders must review the government's submissions *ex parte* and *in camera* "upon request of the government"; this language could be construed to foreclose independent consideration by the court of the constitutional ramifications of denying the NSL recipient access to the evidence that is said to support a gag order. *But see Doe v. Gonzales*, 500 F.Supp.2d 423-24 (construing statute more narrowly). Third, the statutes provide that courts that hear challenges to gag orders must seal documents and close hearings "to the extent necessary to prevent an unauthorized disclosure of a request for records"; this language could be construed to divest the courts of their constitutional responsibility to decide whether documents should be sealed or hearings should be closed. *But see Doe v. Gonzales*, 500 F.Supp.2d 423-24 (finding that statute "in no way displaces the role of the court in determining, in each instance, the extent to which documents need to be sealed or proceedings closed and does not permit the scope of such a decision to made unilaterally by the government").

[8] Documents obtained by the ACLU through the FOIA indicate that the Defense Department believes it has authority to request voluntary disclosure of the same information. *See* http://www.aclu.org/safefree/nationalsecurityletters/32140res20071011.html, at 60-61.

[9] 12 U.S.C. § 3414(d).

[10] Still another statute, 50 U.S.C. § 436 empowers "any authorized investigative agency" to compel financial institutions and consumer reporting agencies to disclose records about agency employees.

Most NSLs are issued by the FBI under 18 U.S.C. § 2709,[11] which was originally enacted in 1986 as part of the Electronic Communications Privacy Act ("ECPA").[12] Since its enactment, the ECPA NSL statute has been amended several times. In its current incarnation, it authorizes the FBI to issue NSLs compelling "electronic communication service provider[s]" to disclose "subscriber information," "toll billing records information," and "electronic communication transactional records."[13] An "electronic communication service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications."[14]

Because most NSLs are issued under ECPA, this testimony focuses on that statute. All of the NSL statutes, however, suffer from similar flaws.

The ECPA NSL statute implicates a broad array of information, some of it extremely sensitive. Under the statute, an Internet service provider can be compelled to disclose a subscriber's name, address, telephone number, account name, e-mail address, and credit card and billing information. It can be compelled to disclose the identities of individuals who have visited a particular website, a list of websites visited by a particular individual, a list of e-mail addresses with which a particular individual has corresponded, or the e-mail address and identity of a person who has posted anonymous speech on a political website. As the *Library Connection* case shows, the ECPA NSL statute can also be used to compel the disclosure of library patron records.[15] Clearly, all of this information is sensitive. Some of it is protected by the First Amendment.[16]

Because NSLs can reach information that is sensitive, Congress originally imposed stringent restrictions on their use. As enacted in 1986, the ECPA NSL statute permitted the FBI to issue an NSL only if it could certify that (i) the information sought was relevant to an authorized foreign counterintelligence investigation; and (ii) there were specific and articulable facts giving reason to believe that the subject of the NSL was a foreign power or foreign agent.[17] Since 1986, however, the reach of the law has been extended dramatically. In 1993, Congress relaxed the individualized suspicion

---

[11] Dep't of Justice, Office of Inspector General, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (March 2008), http://www.usdoj.gov/oig/special/s0803b/final.pdf (hereinafter "2008 OIG Report"), at 107 .

[12] *See* Pub L. No. 99-508, Title II, § 201(a), 100 Stat. 1848 (Oct. 21, 1986) (codified as amended at 18 U.S.C. § 2510, *et seq.*

[13] 18 U.S.C. §§ 2709(a) & (b)(1).

[14] *Id.* § 2510(15).

[15] *Library Connection*, 386 F.Supp.2d at 70.

[16] *See, e.g.. McIntyre v. Ohio Elections Comm.*, 514 U.S. 334, 341-42 (1995) ("[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."); *Talley v. California*, 362 U.S. 60, 64 (1960) ("Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names.").

[17] 18 U.S.C. § 2709 (1988).

requirement, authorizing the FBI to issue an NSL if it could certify that (i) the information sought was relevant to an authorized foreign counterintelligence investigation; and (ii) there were specific and articulable facts giving reason to believe that *either* (a) the subject of the NSL was a foreign power or foreign agent, *or* (b) the subject had communicated with a person engaged in international terrorism or with a foreign agent or power "under circumstances giving reason to believe that the communication concerned international terrorism."[18] In 2001, Congress removed the individualized suspicion requirement altogether and also extended the FBI's authority to issue NSLs in terrorism investigations. In its current form, the NSL statute permits the FBI to issue NSLs upon a certification that the records sought are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."[19]

The relaxation and then removal of the individualized suspicion requirement has resulted in an exponential increase in the number of NSLs issued each year. According to an audit conducted by the Justice Department's OIG, the FBI's internal database showed the FBI issued 8,500 NSL requests in 2000, the year before the Patriot Act eliminated the individualized suspicion requirement.[20] By comparison, the FBI issued 39,346 NSL requests in 2003; 56,507 in 2004; 47,221 in 2005; and 49,425 in 2006.[21] These numbers, though high, substantially understate the number of NSL requests actually issued, because the FBI has not kept accurate records of its use of NSLs. The OIG sampled 77 FBI case files and found 22 percent more NSL requests in the case files than were recorded in the FBI's NSL database.[22]

The statistics and other public information make clear that the executive branch is now using NSLs not only to investigate people who are known or suspected to present threats but also – and indeed principally – to collect information about innocent people.[23] News reports indicate that until very recently the FBI used NSLs "to obtain data not only on individuals it saw as targets but also details on their 'community of interest' – the network of people that the target was in contact with."[24] Some of the FBI's

---

[18] Pub. L. 103-142, 107 Stat. 1491 (Nov. 17, 1993).

[19] 18 U.S.C. § 2709(a) & (b)(1) (2006).

[20] *See* Dep't of Justice, Office of Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters (March 2007), http://www.usdoj.gov/oig/special/s0703b/final.pdf (hereinafter "2007 OIG Report"), at xvi.

[21] *See id.* at xix; 2008 OIG Report at 9.

[22] 2007 OIG Report at 32.

[23] The statistics also make clear that the FBI is increasingly using NSLs to seek information about U.S. persons. The percentage of NSL requests generated from investigations of U.S. persons increased from approximately 39% of NSL requests in 2003 to approximately 57% in 2006. 2008 OIG Report at 9.

[24] Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, New York Times, Sept. 9, 2007; *see also* Barton Gellman, *The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, Washington Post, Nov. 6, 2005 (reporting that

investigations appear to be nothing more than fishing expeditions. As noted above, the ACLU has represented two entities that were served with NSLs. In both cases, the FBI abandoned its demand for information after the NSL recipient filed suit; that is, in both cases the FBI withdrew the NSL rather than try to defend the NSL to a judge. The agency's willingness to abandon NSLs that are challenged in court clearly raises questions about the agency's need for the information in the first place.

The ACLU believes that the current NSL statutes do not appropriately safeguard the privacy of innocent people. H.R. 3189 would significantly improve the current statutes by replacing the requirement that the FBI certify "relevance" with a requirement that the FBI certify individualized suspicion. Specifically, the bill would provide that "[a] national security letter may not be issued unless the official having authority under law to issue such a letter certifies that there are specific and articulable facts giving reason to believe that the information or records sought by that letter pertain to a foreign power or agent of a foreign power."[25] The ACLU believes that this change would protect the privacy of innocent people without impairing the government's ability to compel the production of information about people known or suspected to pose threats.

II. The NSL statutes allow the FBI to impose gag orders without meaningful judicial review.

A second problem with the NSL statutes is that they empower executive agencies to impose gag orders that are not subject to meaningful judicial review.[26] Until 2006, the ECPA NSL statute categorically prohibited NSL recipients from disclosing to any person that the FBI had sought or obtained information from them.[27] Congress amended the statute, however, after a federal district court found it unconstitutional.[28] Unfortunately, the amendments made in 2006, while addressing some problems with the statute, made the gag provisions even more oppressive. The new statute permits the FBI to decide on a case-by-case basis whether to impose gag orders on NSL recipients but strictly confines the ability of NSL recipients to challenge such orders in court.

As amended, the NSL statute authorizes the Director of the FBI or his designee (including a Special Agent in Charge of a Bureau field office) to impose a gag order on any person or entity served with an NSL.[29] To impose such an order, the Director or his designee must "certify" that, absent the non-disclosure obligation, "there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic

---

the FBI apparently used NSLs to collect information about "close to a million" people who had visited Las Vegas).

[25] H.R. 3189, § 3(a).

[26] All of the NSL statutes authorize the imposition of such gag orders.

[27] 18 U.S.C. § 2709 (2005).

[28] *Doe v. Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004).

[29] 18 U.S.C. § 2709(c).

relations, or danger to the life or physical safety of any person."[30] If the Director of the FBI or his designee so certifies, the recipient of the NSL is prohibited from "disclos[ing] to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the [FBI] has sought or obtained access to information or records under [the NSL statute]."[31] Gag orders imposed under the NSL statute are imposed by the FBI unilaterally, without prior judicial review. While the statute requires a "certification" that the gag is necessary, the certification is not examined by anyone outside the executive branch. No judge considers, before the gag order is imposed, whether secrecy is necessary or whether the gag order is narrowly tailored.

The gag provisions permit the recipient of an NSL to petition a court "for an order modifying or setting aside a nondisclosure requirement."[32] However, in the case of a petition filed "within one year of the request for records," the reviewing court may modify or set aside the nondisclosure requirement only if it finds that there is "no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person." *Id.* § 3511(b)(2). Moreover, if a designated senior government official "certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations," the certification must be "treated as conclusive unless the court finds that the certification was made in bad faith." *Id.*[33]

As the district court found in *Doe v. Gonzales*, the amended gag provisions are unconstitutional. The amended statute violates both the First Amendment and the principle of separation of powers because it forecloses courts from assessing individual gag orders under "strict scrutiny," the constitutionally mandated standard of review. As the court explained:

> [T]he standard of review prescribed in [18 U.S.C.] § 3511(b) is sharply at odds with the standard of review the Supreme Court has explicitly held is required to assess the conformance of a statute with the strictures of the First Amendment. Congress cannot legislate a constitutional standard of review that contradicts or supercedes what the courts have determined to be the standard applicable under the First Amendment for that purpose.

---

[30] *Id.* § 2709(c)(1).

[31] *Id.*

[32] *Id.* § 3511(b)(1).

[33] In the case of a petition filed under § 3511(b)(1) "one year or more after the request for records," the FBI Director or his designee must either terminate the non-disclosure obligation within 90 days or recertify that disclosure may result in one of the enumerated harms. *Id.* § 3511(b)(3). If the FBI recertifies that disclosure may be harmful, however, the reviewing court is required to apply the same extraordinarily deferential standard it is required to apply to petitions filed within one year. *Id.* If the recertification is made by a designated senior official, the certification must be "treated as conclusive unless the court finds that the recertification was made in bad faith." *Id.*

> *See Dickerson v. United States*, 530 U.S. 428, 437, 120 S.Ct. 2326, 147 L.Ed.2d 405 (2000) ("Congress may not legislatively supersede our decisions interpreting and applying the Constitution.") . . . .
>
> [A] statute which constitutes a prior restraint on speech or a content-based restriction on speech must be strictly construed, meaning that it must be narrowly tailored to advance a compelling government interest. That is what the judiciary has said the constitutional law is on this vital principle. Congress, even as an accommodation to the executive branch on matters of national security, cannot say that that constitutional standard is something else. That is precisely what § 3511 attempts to do insofar as it decrees the standard of review and level of deference the judiciary must accord to the executive in adjudicating a challenged restriction on protected speech.[34]

The district court rightly found that the gag provisions are unconstitutional for another reason: because they condition NSL recipients' right to speak on the approval of executive officers but fail to provide procedural safeguards to ensure that the censorial power is not abused. Referencing the Supreme Court's decision in *Freedman v. Maryland*, 380 U.S. 51 (1965), the court found that the statute is unconstitutional because it places the burden of initiating judicial review on the would-be speaker – that is, the NSL recipient – rather than the government. The court explained:

> [A]n NSL recipient – an ECSP – will generally lack the incentive to challenge the nondisclosure order in court – as noted by the Supreme Court in *Freedman*. *See* 380 U.S. at 59. Such a challenge would be time consuming and financially burdensome, and . . . the NSL recipient's business does not depend on overturning the particular form of restriction on its speech. That NSL recipients generally have little or no incentive to challenge nondisclosure orders is suggested by empirical evidence. Although the FBI issued 143,074 NSL requests from 2003 to 2005 alone . . . only two challenges have been made in federal court since the original enactment of the statute in 1986.[35]

The district court found, in sum, that the statute invests the FBI with sweeping censorial authority but fails to provide procedural safeguards that the Constitution requires.

Congress presumably enacted the gag provisions to allow the executive branch to protect information whose disclosure would jeopardize national security. Because the NSL statutes fail to provide constitutionally required procedural safeguards, however, and because gag orders are not subject to meaningful judicial review, the executive can use the gag provisions not only to protect sensitive information but to silence critics of the government's surveillance activities. The ACLU's client in *Doe v. Mukasey* has said

---

[34] *Doe v. Gonzales*, 500 F.Supp.2d at 411-12.

[35] *Id.* at 405.

in an affidavit (and in an Op-Ed that was published in the *Washington Post*), that he suspects that the NSL served on him was illegal and that the FBI was seeking information to which the agency was not entitled. The gag order prevents Doe, however, from explaining why he holds this opinion and even from disclosing his own identity. Notably, the FBI continues to enforce the gag order even though the FBI abandoned its demand for records over a year ago, and even though the underlying investigation began at least four years ago and may well have ended.[36]

The FBI's sweeping power to silence NSL recipients also deprives the public – and Congress – of the information it needs in order to evaluate the wisdom and effectiveness of government policy. The ACLU's client in *Doe v. Mukasey* has explained that the gag order prevented him from disclosing information that might have influenced the debate about whether the Patriot Act should be reauthorized. He has explained:

> I found it particularly difficult to be silent about my concerns [about the NSL statute] while Congress was debating the reauthorization of the Patriot Act in 2005 and early 2006. If I hadn't been under a gag order, I would have contacted members of Congress to discuss my experiences and to advocate changes in the law. The [2007 OIG] report confirms that Congress lacked a complete picture of the problem during a critical time: Even though the NSL statute requires the director of the FBI to fully inform members of the House and Senate about all requests issued under the statute, the FBI significantly underrepresented the number of NSL requests in 2003, 2004 and 2005, according to the report.[37]

The ACLU's clients in *Library Connection v. Gonzales* were also prevented from sharing critical information with the public and Congress. In striking down the gag order imposed on Library Connection, the court observed that the gag order stifled debate about an issue of pressing public concern:

> The statute has the practical effect of silencing those who have the most intimate knowledge of the statute's effect and a strong interest in advocating against the federal government's broad investigative powers pursuant to [the NSL statute]: those who are actually subjected to the governmental authority by imposition of the non-disclosure provision. The government may intend the non-disclosure provision to serve some purpose other than the suppression of speech. Nevertheless, it has the practical effect of silencing those individuals with a constitutionally protected interest in speech and whose voices are particularly important to an ongoing, national debate about the intrusion of governmental authority into individual lives.[38]

---

[36] John Doe, *My National Security Letter Gag Order*, Washington Post, March 23, 2007.

[37] John Doe, *My National Security Letter Gag Order*, Washington Post, March 23, 2007.

[38] *Library Connection v. Gonzales*, 386 F.Supp.2d 66, 75 (D.Conn. 2005).

The ACLU believes that H.R. 3189 would remedy the serious constitutional problems with the current gag provisions. While the bill would impose a 30-day gag order on anyone served with an NSL, the non-disclosure obligation would expire at the end of the 30-day period unless the FBI affirmatively sought an extension from "the district court of the United States in any district within which the authorized investigation that is the basis for a request pursuant to this section is being conducted."[39] The application for an extension would have to "state specific and articulable facts giving the applicant reason to believe that disclosure that the [FBI] has sought or obtained access to information or records under this section will result in (A) endangering the life or physical safety of any person; (B) flight from prosecution; (C) destruction or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously endangering the national security of the United States by alerting a target, a target's associates, or the foreign power of which the target is an agent, of the Government's interest in the target."[40] The court would be permitted to grant the extension "if the court determines that the order is narrowly tailored to meet a compelling interest and that there is reason to believe that disclosure that the [FBI] has sought or obtained access to information or records under this section will have one of the [statutorily specified] results."[41] The bill would permit the FBI to "renew[]" the non-disclosure obligation for "additional periods of not more than 180 days upon another application meeting the [same] requirements."[42]

The ACLU believes that H.R. 3189 would provide greater protection for the First Amendment rights of NSL recipients – and allow greater public oversight of the government's use of NSLs – while allowing for limited secrecy in those investigations that actually require such secrecy.

III. Publicly available information about the government's use of NSLs makes clear that there is a pressing need for the amendments proposed by H.R. 3189.

The 2006 amendments to the NSL statutes required the Department of Justice OIG to audit the FBI's use of NSLs. The first of these audits, covering 2003 through 2005, was released in March 2007. The audit found that the FBI had substantially underreported to Congress the number of NSLs it had issued; that in some cases the FBI issued NSLs even where no underlying investigation had been approved; that some NSL recipients had provided the FBI with information to which the agency was not entitled, including voicemails, emails, and images; and that the FBI issued more than 700 so-called "exigent letters," which were authorized neither by the NSL statute nor by any other law, and some of which were not related to any authorized investigation.

---

[39] H.R. 3189, § 3(d)(3) & (4).

[40] *Id.* § 3(d)(5).

[41] *Id.* § 3(d)(6).

[42] *Id.* § (d)(7). The bill would allow for disclosures, even during the term of the gag order, to "those persons to whom disclosure is necessary in order to comply with an order under this section" and "an attorney in order to obtain legal advice regarding such order." H.R. 3189, § 3.

In March 2008, the OIG issued an audit covering 2006 and evaluating the reforms implemented by the DOJ and the FBI after the release of the 2007 OIG Report. The audit found, among other things, that the FBI could not locate supporting documentation for 15% of NSLs; that the FBI diminished the seriousness of violations of internal controls and regulations by characterizing them as "administrative errors"; that even by the FBI's count there had been more than 600 potential violations that should have been reported to the Intelligence Oversight Board (IOB); that an incredible 71.5% of NSLs issued from FBI headquarters (as opposed to NSLs issued from field offices) involved violations that should have been reported to the IOB; that the FBI could not locate return information for more than 500 NSL requests; that in several cases the FBI collected private information regarding innocent people who were not connected to any authorized investigation, entered the information into case files, and/or uploaded it into FBI databases; and that the FBI improperly issued "blanket NSLs" to "cover information already acquired through exigent letters and other informal responses."[43] The blanket letters sought information on 3,860 telephone numbers.[44]

One of the most troubling of the OIG's findings was that the FBI had used an NSL to circumvent the statutory prohibition against investigations based solely on First Amendment activity. While the relevant portion of the OIG's report is heavily redacted, it appears that sometime in 2006 the FBI twice applied to the FISA Court for an order under 50 U.S.C. § 1861 to compel the disclosure of "tangible things."[45] The FBI submitted these applications even though lawyers in the Office of Intelligence Policy and Review had expressed concern that the underlying investigations raised issues under the First Amendment.[46] The court ultimately denied the applications, both times finding that the FBI had not provided a sufficient factual basis for the order and that the request "implicated the target's First Amendment rights."[47] Rather than abandon its effort to obtain the tangible things, however, the FBI appears to have sought the same materials with NSLs – instruments which are of course not subject the FISA Court's review.[48] Asked why the FBI had issued the NSLs after the FISA court's rejection of the "tangible things" applications, the FBI's General Counsel stated that "she disagreed with the court's ruling and nothing in the court's ruling altered her belief that the investigation was appropriate."[49]

---

[43] 2008 OIG Report at 123.

[44] Dep't of Justice, Office of Inspector General, A Review of the FBI's Use of Section 215 Orders for Business Records in 2006 (March 2008), http://www.osdoj.gov/oig/special/s0803a/final.pdf (hereinafter "2008 Section 215 Report"), p.123.

[45] *Id.* at 68.

[46] *Id.* at 67.

[47] *Id.* at 68.

[48] *Id.* at 72.

[49] *Id.* at 72; *see also id.* at 71 n.63.

The 2008 OIG Report also documents abuses of the gag provisions. According to the OIG, the FBI imposed gag orders on 97% of NSL recipients despite internal guidance stating that such orders "should not be made in a perfunctory manner" and should "no longer [be] automatically included in the NSL."[50] The OIG also found that some NSLs that imposed gag orders did not contain sufficient explanation to justify imposition of the gag orders, and that the FBI improperly imposed gag orders in eight of eleven "blanket" NSLs that senior FBI officials issued to cover illegal requests made through "exigent" letters.[51]

The OIG's reports document abuses by the FBI, but the ACLU has obtained records through the Freedom of Information Act that also suggest abuse of NSLs by other agencies. The records show that the Defense Department ("DoD") has issued hundreds of NSLs since September 2001 to obtain financial and credit information, and – more troubling still – that DoD has asked the FBI to issue NSLs in DoD investigations, a practice that may have allowed DoD to access records that it would not have been able to obtain under its own NSL authority. Only the FBI has the statutory authority to issue mandatory NSLs for electronic communication transaction records and certain consumer information from consumer reporting agencies. DoD's practice of relying on the FBI to issue NSLs allows DoD to circumvent statutory limits on its own investigatory powers.[52]

It is possible that some of the abuses documented in the OIG reports and in the FOIA documents could be addressed through stronger internal controls and regulations. Notably, the OIG found that the FBI had not fully implemented all of the recommendations made in the 2007 OIG Report.[53] While stronger internal controls and regulations could make a difference at the margin, however, the main problem is not the absence of those controls but the sweep of the NSL statutes themselves. There is no way to address the problems with the NSL powers without amending the NSL statutes themselves.

* * *

The ACLU strongly supports the Subcommittee's efforts to amend the NSL statutes. As explained above, the statutes invest the FBI with sweeping power to collect information about innocent people and to silence those who are compelled to disclose the information. The ACLU believes that H.R. 3189 would provide needed safeguards for individual rights while at the same time accommodating the executive's legitimate interest in collecting information about foreign power and foreign agents.

Thank you for giving us the opportunity to provide our views.

---

[50] 2008 OIG Report at 124.

[51] *Id.* at 127.

[52] Some of the records that were made public are available at http://www.aclu.org/safefree/nationalsecurityletters/32140res20071011.html.

[53] 2008 OIG Report at 15.

Mr. NADLER. I thank the gentleman.

And I now recognize Mr. Fein for 5 minutes.

TESTIMONY OF BRUCE FEIN, CHAIRMAN OF THE AMERICAN FREEDON AGENDA, FORMER ASSISTANT DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. FEIN. Thank you, Mr. Chairman and Members of the Subcommittee.

I would like to begin with some cardinal principles about the United States Constitution and the theory of government itself, that I think should inform the relative balance between law enforcement and privacy that is at issue in discussing National Security Letters.

John Adams remarked that the fuel of the American Revolution was James Otis' protest against King George III's customs collectors invading every home in search of contraband or otherwise. It was a privacy issue that was the heart of the American Revolution.

And the idea that was descendent was that the right to be left alone from government intrusions, as Justice Louis Brandeis explained, is the most cherished amongst civilized people—the right to be left alone. It did not mean the government could never intercede—there are obviously problems with many mischievous people in the community—but that the government had to make a very powerful case to show why that right to be left alone should be disturbed.

Moreover, the Founding Fathers believed not that government should be weak, but that in exerting aggressive powers, there should be checks and balances. This is an idea that was explained by Justice Robert Jackson in *United States v. Johnson*.

Now, Jackson spoke from some experience. He was the Nuremberg prosecutor. He had seen the Nazis first hand.

And he explained that, what the police often fail to remember is not that the law is against detecting criminals, but that the decisions to make intrusions on privacy need to be checked and supervised by an outside party—there, a judge issuing a judicial warrant—drawing inferences based from a neutral perspective, rather than from the perspective, as Justice Jackson put it, the competitive enterprise of seeking to punish and capture criminals.

That is the background in which we come to approach the National Security Letters. The right to be left alone is cherished. The burden is on the government to show why these rights should be invaded; and moreover, if so, why there should not be customary checks and balances.

Let me outline what are the ways in which traditionally we try to check aggressiveness or needless intrusion on the right to privacy.

First, with a grand jury, those are citizens who decide whether to issue a subpoena for records that are the type that are sought in National Security Letters. And the grand jury is overseen by a judge, an Article III judge.

Moreover, as pointed out, typically the subpoena is subject to disclosure in the sunshine. We know, as Louis Brandeis said, sunshine is the best disinfectant. So, that publicity is an additional deterrent to wrongdoing or misuse.

Now, the National Security Letters fall outside that customary framework that balances privacy against law enforcement. There is no outside party that reviews the issuance of National Security Letters. It is the FBI deciding on its own. Moreover, with the nondisclosure rule, you do not have the sunshine that can act as a deterrent, as well.

Now, it has been observed correctly, I think, by Congressman Franks in the previous exchanges, that certainly, National Security Letters, if you look, have they produced useful information? Certainly, they have.

But the decisive issue, I think, for the Committee is, why couldn't that information have been obtained through a customary grand jury proceeding or gathering intelligence under FISA, where typically you have a judge decide whether or not there is sufficient reason to intrude upon that cherished right to be left alone?

And I do not think the FBI has been able to explain what it is that they got with National Security Letters that they could not possibly have gotten, had they used the regular way that the Founding Fathers thought was sufficient.

I think that, when you ask about internal reviews, let us remember FISA. That was a warrantless national security program which had internal reviews every 45 days. And mirabile dictu, every 45 days it was approved.

These kinds of internal checks do not work. I worked in the Department of Justice. You do not need to have an explicit order in the bureaucracy to know which way it will come out. And we have seen that in some respects, I think, between the lines, if you read John Yoo's unclassified document relating to what was torture and what was not, whether the President had supreme commander-in-chief authority to flout any law this body enacted in the name of national security.

And that is what the Founding Fathers understood. If men were angels, we would not need separation of powers. But they relied upon checks and balances. As President Reagan put it, "Trust, but verify."

And I think that is the spirit of Congressman Nadler's bill, and I highly support it and commend it.

Thank you.

[The prepared statement of Mr. Fein follows:]

PREPARED STATEMENT OF BRUCE FEIN

Mr. Chairman and Members of the Subcommittee:

I welcome the opportunity to share my views on H.R. 3189, the National Security Letters Reform Act of 2007. I support the bill. It strikes a balance between privacy and law enforcement vastly superior to existing law in honoring the charter principles of the American Revolution and the Constitution.

The Declaration of Independence sets forth the purpose of the United States government: to secure the unalienable rights to life, liberty, and the pursuit of happiness enjoyed by ever y American citizen. The signature creed of the United States has been that individual freedom is the rule. Government intrusions are the exception that can be justified only by clear and substantial community interests. Justice Louis D. Brandeis lectured in *Olmstead v. United States* (1928) that the right to be left alone is the most cherished freedom among civilized people. Privacy is not only a good in itself; it also nurtures a sense of assertiveness, robust independence, and even rebelliousness which are the lifeblood of democracy. The greatest danger to freedom is an inert or docile people fearful that the government has access to every detail of their private lives.

In the typical federal criminal investigation, a grand jury composed of ordinary citizens, supervised by an independent and neutral federal judge, issues subpoenas for records relevant to determining whether an indictment should be voted. The prosecutor cannot act as a surrogate for the collective view of the grand jury because of the temptation to overreach in a quest for fame, vindictiveness or otherwise. Supreme Court Justice Robert Jackson captured the idea in *Johnson v. United States* (1948) in addressing the Fourth Amendment's protection against unreasonable searches and seizures and the customary requirement of a judicial warrant based on probable cause: "Its protection consists in requiring inferences [of crime] be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime."

The recipient of a grand jury demand may move to quash the subpoena as unconstitutional or otherwise in violation of law. The target may also publicize the subpoena to expose possible abuse or overreaching or the need for remedial legislation. Sunshine is frequently the best disinfectant.

Of course, there are exceptions to every rule. The Constitution is not a suicide pact. It seems worth noting, however, that the United States Supreme Court has refused to carve out a Fourth Amendment exception for murder investigations despite the alarming annual number of murders. (The FBI estimated the murder toll in 2006 at more than 17,000, or approximately six times 9/11 fatalities). National security letters (NSLs), which deviate sharply from customary law enforcement methods, might be justified in principle if there were a substantial showing that espionage or international terrorism crimes were eluding detection because available investigatory tools were insufficiently muscular; and, that NSLs would provide the necessary muscle to thwart national security crimes. (The Patriot Act's elimination of the wall between intelligence collection and law enforcement makes NSL requests indistinguishable from grand jury subpoenas for documents), NSLs should are presumptively disfavored because they may be issued by the government without any citizen or judicial supervision and lack the transparency that is a cornerstone deterrent to abuses.

I do not believe either benchmark for NSLs has ever been satisfied to overcome the presumption. Before their enshrinement in the Patriot Act, Congress was not presented with a roster of international terrorist incidents that probably would have been foiled if NSLs had been available. The 9/11 Commission did not find that the terrorist abominations might have been forestalled with NSLs. After years of intensive use, this Committee has not been presented with a list of espionage or international terrorism crimes that were prevented or solved because of NSLs and could not have been prevented or solved otherwise. NSLs are the twin of the quest to emasculate the individual warrant protection of the Foreign Intelligence Surveillance Act with general warrants rubber stamped after the fact by a FISA judge.

H.R. 3189 should be supported because it diminishes (although it does not eliminate) the gratuitous encroachments on citizen privacy under the existing laws governing NSLs. There is not a crumb of hard evidence that enactment of the bill would cause a single act of planned espionage or international terrorism to go undetected.

The bill would confine NSLs to investigations where there are specific and articulable facts indicating the target is a foreign agent or foreign power. The former standard was simple relevancy to an espionage or international terrorism investigation. The bill also saddles NSLs with the same standards of reasonableness as would obtain if a grand jury subpoena had been issued in conjunction with an espionage or international terrorism investigation. It also places reasonable limits on the secrecy of NSLs. The democratic values advanced by transparency cannot be overstated. Secret government wars with self-government and deterring misconduct. The Constitution does not permit secret detentions and trials of suspected international terrorists even if public knowledge might clue Al Qaeda where its network might be vulnerable. Of course, a disclosure of an NSL to assist obstruction or evasion of justice is itself a crime.

The bill would require minimization procedures to diminish the volume of private information unrelated to foreign intelligence or crime in government files. The standards for retention, however, are inescapably nebulous, and will easily blunt the purpose of minimization as they have regarding FISA. Deterrence of government wrongdoing is buttressed by creating a criminal justice suppression remedy for violations and a civil cause of action for the target. Regarding the latter, I would bring the suit within the universe of civil rights claims subject to the Civil Rights Attorneys' Fees Award Act of 1988. The recipients of NSLs have little or no incentive to challenge their legality because compliance with an administrative subpoena ordinarily shields the recipient from liability to the target. See e.g., 18 U.S.C. 2703(e).

Freedom requires a certain level of risk that tyrannies might find unacceptable. The risk of international terrorism in China may be less than in the United States, but who among us would prefer the former to the latter? We should never forget that the revolutionary idea of America was that government exists to secure the unalienable individual rights of every citizen period, with no commas, semi-colons or question marks. There can be no doubt that NSLs have been fueled by post-9/11 fears. But we should be steeled against capitulation by James Madison's admonition: "If Tyranny and Oppression come to this land, it will be in the guise of fighting a foreign enemy."

Mr. NADLER. I thank the gentleman.

I recognize Mr. Woods for 5 minutes.

TESTIMONY OF MICHAEL J. WOODS, FORMER CHIEF, FBI NATIONAL SECURITY LAW UNIT

Mr. WOODS. Thank you, Mr. Chairman, Mr. Franks and Members of the Committee.

I am very pleased to have been invited to this hearing this afternoon to assist you.

My interest in this area is really twofold.

First, I was, as chief of national security law in the FBI prior to the PATRIOT Act and shortly thereafter, supervising the lawyers, who at that time prepared National Security Letters. I have calculated roughly that 75 to 80 percent of them were prepared within 10 or 15 feet of my office where I sat. So, I am happy to give the Committee the benefit of that experience.

I was also part of the discussion and part of the process, at least in the FBI, of making proposals at the time for the PATRIOT Act. And so, I can explain, if the Committee is interested, the background and the change in legal standard.

But I am also fascinated from an academic perspective since, with the idea of transactional information. We all generate enormous amounts of this. And technology and the changes in our society are increasing the amount of that information. And although it does not contain the content of private communication, it is revealing a steadily more detailed picture of what we do every day.

That information—unlike our content, unlike things that we have a more direct privacy interest in—resides in the hands of third parties in quantities, formats and conditions of which most of us remain unaware. The constant expansion in the capacity of storage systems and in the power of search engine technology makes this transactional information more permanent—and more easily accessible—than ever before.

So, the question is: Under what circumstances do we want the government in its intelligence gathering function to have access to that information? How should they use it? How should they store it?

How can their use of it be challenged? How can their acquisition of it be challenged? And I am hoping that I can contribute something to the Committee's discussion of that today.

It is an enormous challenge. On the one hand, the explosion of transactional information has opened a new front in the fight against terrorism and foreign intelligence services. Our very sophisticated adversaries have long since learned to conceal their direct communications from us, but now may be detected in their digital footprint.

After 9/11, transactional information was key to reconstructing the terrorists' operations, and it is probably one of our best hopes, one of our most effective means of detecting another imminent attack.

Yet, this information, as I say, is revealing more than just the transaction, just the outside nature. Its quantity and quality are raising the amount that it tells us about a subject.

And so, I believe that the tool that the FBI has to acquire that information, though it must be flexible and it must be efficient, and it must, as it does now, allow the acquisition of information relevant to an investigation, it needs to be controlled. It needs to have effective minimization rules, effective retention rules.

And beyond the sort of legal effectiveness or legal elegance of them, they have to be rules that inspire confidence in the American public, confidence that this authority is under control, confidence that it is being used correctly.

My hope is to contribute to that discussion today with the Committee, and I am very happy to answer any questions.

[The prepared statement of Mr. Woods follows:]

PREPARED STATEMENT OF MICHAEL J. WOODS

SUBCOMMITTEE ON THE CONSTITUTION, CIVIL RIGHTS, AND CIVIL LIBERTIES

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES

HEARING ON H.R. 3189, THE "NATIONAL SECURITY LETTERS REFORM ACT OF 2007"

April 15, 2008

Testimony of Michael J. Woods

Mr. Chairman and members of the Sub-committee: I am very pleased to have an opportunity to appear before you this afternoon. As one of a very small group of people who have both an academic interest in and substantial practical experience with national security letters, I am happy to offer both my research and my FBI experiences as resources for the Committee.

Like the other witnesses this afternoon and, I am sure, members of the Committee, I see in the constantly-evolving digital environment an enormous challenge for our government. Each of us now generates an increasing large and complex body of digital information in the course of our daily lives. Every time we communicate using an electronic device, reach out for information on the Internet, and nearly always when we make a purchase, we leave behind a digital record of our activity. The simple act of walking around with a cell phone or other wireless device in your pocket can create digital footprints since that device constantly transmits and receives operating signals. Taken together, this cloud of transactional information, though it does not contain the content of our private communications, reveals a steadily more detailed picture of our daily activities, personal habits and social networks. This information largely resides in the custody of third parties, in quantities, formats and conditions of which most of us are unaware. The constant expansion in the capacity of storage systems and in power of search engine technology makes this transactional information more permanent, and more easily accessible, than ever before.

The challenge presented by this environment is particularly acute in the area of counterintelligence and counter-terrorism. On the one hand, the explosion of transactional information has opened a new front in the fight against terrorists and foreign intelligence services. Sophisticated adversaries that have long since learned to conceal their direct communications may be detected by their digital footprints. After the 9/11 attacks, we used transactional information to reconstruct quickly the details of terrorists'

operation. Suspicious transactions are likely to be one of the more effective means of detecting an imminent attack or the existence of a new terrorist cell. On the other hand, the compromise of privacy by the acquisition of transactional data seems greater now that the quantity and detail of that information has increased. Under what circumstances should the government be able to access this information? What standards for the handling and retention of such information should apply to the government? Even assuming proper implementation within the FBI, do the current forms of the national security letter statutes adequately answer these concerns? My hope is to contribute something to your discussion of these questions today.

I would like to begin by offering my perspective on the development of the national security letter statutes over the years, with particular emphasis on the evolution of the legal standards embodied in those statutes. What I am offering here is really a summary of much more detailed material that I have published in an article in the Journal of National Security Law & Policy. I have submitted a copy of the full article as an attachment to my written testimony and it is also available on the Journal's website at http://www.mcgeorge.edu/documents/publications/jnslp/03_Woods_Master.pdf. I will follow this background narrative with observations from my direct experience with the national security letter process in the FBI and, finally, some thoughts on the revision of these authorities.

The legal authorities that we now refer to as "national security letters" were, in their origin, not the result of any carefully considered plan. Rather, they were ad hoc responses to legislative developments – responses that were intended simply to enable the FBI's national security components to keep doing what they had been doing previously. Up through the 1970s, FBI counterintelligence agents who needed transactional records held by third parties (bank records, telephone toll records, etc.) simply asked for them. This was sometimes done in a formal letter stating that the materials were needed for national security reasons. The term "national security letter" actually derives from this older practice, and not from the statutes themselves. In 1976, the Supreme Court, in United States v. Miller ruled that financial records held by a bank were not protected by the account holder's Fourth Amendment protections and later made a similar ruling with respect to telephone records (Smith v. Maryland in 1979). Subsequent to these decisions, Congress enacted statutory protections for financial information (in the Right to Financial Privacy Act of 1978), telecommunications data (the Electronic Communications Privacy Act in 1986), and credit information (through various amendments to the Fair Credit Reporting Act).

One effect of these new laws was to limit the ability of third-party record holders to honor the FBI's informal "national security letter" requests. Accordingly, the FBI sought language in the three relevant statutes that would enable it to issue letters to record-holding third parties requiring the production of transactional records without notification of the person to whom the record pertained. Eventually, each of these statutes were amended to allow production to the FBI upon a certification that there existed "specific and articulable facts giving reason to believe" that the target was (or, in some cases, had been a person in contact with) an "agent of a foreign power," as defined

in the Foreign Intelligence Surveillance Act. With a few minor technical modifications, these statutes were the authority for FBI national security letters up until the passage of the USA PATRIOT Act in 2001.

I think there are several features of pre-Patriot Act NSLs that merit attention here. The first is the unusual legal standard employed. "Specific and articulable facts giving reason to believe" was a largely undefined legal standard when it was integrated into these statutes. Unlike the standard of "probable cause" or "relevance," it is not used elsewhere in criminal law and has no body of jurisprudence to explain it. The inspiration for this standard appears to have been the then relatively new Executive Branch oversight rules for the intelligence community, in particular the language of the Attorney General Guidelines for FBI Foreign Counterintelligence Investigations (or "FCI Guidelines") mandated by Executive Order 12,333. The essential language of those Guidelines was, and remains, classified, but the legislative history of NSL statutes strongly implies that the "specific and articulable facts" standard corresponded to Attorney General guideline language. The NSL language (and presumably the language of the Guidelines) reflected the nature of contemporary FBI national security operations. Prior to the late 1990s, those operations were dominated by traditional counterintelligence. The FBI's principal counterintelligence function was to keep tabs on foreign intelligence officers operating inside the United States and to detect any spies that those operatives may have recruited. Counter-terrorism was, of course, a concern of the FBI at the time, but was, until the 1990s, seen as a relatively small subset of traditional counterintelligence (a fact reflected in the FBI's organizational structure during this era). In the 1990s, of course, this relationship was inverted, with counter-terrorism functions eventually coming to equal, and then surpass, counterintelligence. My point is that the "specific and articulable facts" standard was particularly suited to the counterintelligence operations of the era in which it was created. A FBI counterintelligence investigation involved examining a linear connection between a foreign intelligence officer (about whom much was known) and his contacts (potential spies). The information known about the intelligence officer was specific in nature, and could be readily used to meet the NSL legal standards. The "specific and articulable facts" standard was particularly well suited to the situation in which an agent needed to obtain information about an already identified agent of a foreign power and his contacts.

A second feature of the pre-Patriot Act NSLs was the restricted manner in which they were generated. Between the creation of these authorities and their Patriot Act makeover in 2001, the statutes authorized, at most, about twelve officials in the FBI to sign NSLs. The majority of NSLs were, prepared, reviewed and approved within the National Security Law Unit at FBI Headquarters, with a relatively small number of NSLs prepared in the FBI's New York, Los Angeles, and Washington DC field offices (each of these offices having one of the authorized officials in residence). As Chief of the National Security Law Unit, I oversaw the production and approval of NSLs. The NSLs were prepared by a handful of analysts in my office, whose principal duty was to master this process. The attorneys who reviewed the NSLs, either in my office or in the three designated field offices, were specialists in national security law. In short, NSLs were produced and reviewed by a relatively small group of people, all of whom had substantial

experience with these specific authorities. Under these circumstances, it was possible to monitor directly the quality and accuracy of the NSLs produced. Problems of the sort noted in the recent IG reports were far less likely to occur in that environment.

Finally, the recipients of NSLs in the 1980s and early 1990s differed substantially from those encountered later. Most NSLs were served on a small handful of telecommunications companies that had long-standing relationships with the FBI and were well equipped to comply with compulsory process, whether in the form of criminal subpoenas, surveillance orders, or NSLs. In addition, the transactional information these recipients held was far more limited and predictable in its nature than that encountered today. These recipients understood what an NSL was and knew what they could produce in response. I believe that understanding this background helps to explain the rather underdeveloped form of the original NSL statutes. Given the stable relationship with recipients, there was little perceived need for the statutes to contain clear enforcement mechanisms, detailed definitions, or a means to limit or challenge the secrecy requirements attached to the NSL. The legislative history of these provisions indicates to me that they were relatively simple "fixes," just intended to reconcile pre-existing practices with the new statutory protections. The statutes did not appear to contemplate numbers of NSLs much greater than that experienced at the time, or a recipient base that was more diverse and perhaps less cooperative.

As noted above, the operational environment began to change in the mid to late 1990s. I joined the FBI's National Security Law Unit in 1997, becoming its chief in 1999 and remaining until early 2002. During my tenure, the NSL process experienced increasing stress as a result of changed conditions. The rapid growth in the number of counter-terrorism investigations significantly elevated the demand for NSLs. At the same time, these investigations began to present more complex factual scenarios. Unlike the traditional linear counterintelligence case, in which the foreign agent tried to recruit the domestic spy using infrequent and highly secure forms of communication, many counter-terrorism cases involved complex networks generating a much larger volume of communication and financial transactions. In counter-terrorism cases, the starting point was often not a clearly identifiable agent of a foreign power (as in counterintelligence); indeed, the relevant "foreign power" was itself an imperfectly understood terrorist organization that might defy precise definition. As a consequence, counter-terrorism investigators often had a far more difficult time meeting the "specific and articulable facts" standard. The analysts preparing NSLs often had to send the requests back to the agents multiple times because the information provided did not meet the legal requirements. Many NSLs took months to make it through the process, and many requests were ultimately denied. Though we repeatedly took steps to streamline and improve the production process, the volume of requests continued to overwhelm the available resources.

The NSL process was also beginning to experience difficulties arising from new NSL recipients. By the late 1990s, the FBI had occasion to serve NSLs not just on the traditional telecommunications providers and financial institutions, but also on an ever-expanding number of Internet service providers and other web-based businesses. In so

doing, the FBI encountered recipients who were completely unfamiliar with national security legal authorities. In this environment, the lack in the NSL statutes of clear definitions, enforcement provisions, and judicial review occasionally became an issue. The exponential increase in the amount and detail of retained transactional data also affected the NSL process at this point.

By the time of the 9/11 attacks, I believe there was a widespread perception within the FBI that NSLs were simply too difficult to obtain to be of much operational use, particularly in fast-moving counter-terrorism investigations. The frustration manifested itself in frequent complaints about bottlenecks in the process and calls for broader delegation of signature authority than was allowed by the statutes at the time.

After the 9/11 attacks, I became responsible for preparing the FBI's proposals in the legislative process that would ultimately generate the USA PATRIOT Act. In reference to NSLs, the FBI requested three changes. First, the standard for NSLs was to be changed from "specific and articulable facts" to a standard of simple relevance to a properly authorized investigation (which is the standard used for obtaining the same information in criminal cases). Second, the FBI asked for permission to delegate NSL signature authority to the field office level, so that NSLs could be prepared quickly and locally. Third, the FBI proposed a general administrative subpoena authority that would allow the FBI to obtain business records that did not fall within the specific categories covered by NSLs. Congress essentially adopted the first two proposals into the Patriot Act. The administrative subpoena idea was apparently integrated into the language that became the new Section 215 "Business Records" language in FISA.

In November 2001, the FBI Director delegated NSL signature authority to the field office level. This meant that NSLs could now be prepared, reviewed, and issued independently by each of the FBI's 56 field offices. I drafted the initial legal guidance to the field offices, which contained detailed instructions for the preparation of NSLs, required legal review by the lawyer in each field office (the "Chief Division Counsel" or "CDC"), and contained model NSL documents. In those chaotic months following 9/11, I think that there was a general understanding that the new Patriot Act authorities needed to be deployed as quickly as possible, and that more comprehensive guidance and training would have to wait. This was true, I believe, not just with respect to NSLs, but also with the multitude of other changes that came through the Patriot Act. I would add that during the whole Patriot Act process and thereafter, NSLs were the subject of very little attention, especially in comparison to the higher profile and more volatile FISA issues.

I left FBI headquarters for my position at the National Counterintelligence Executive early in 2002 and my direct experience with the FBI's use of NSLs ended at that point. After reviewing the Inspector General reports, it is obvious to me that the training, comprehensive guidance, and internal controls that were required for the effective implementation of the new NSL authorities and postponed in 2001, simply did not occur until public attention was focused on this issue in late 2005. I have no

particular insight into why that happened, since I had no significant access to the FBI during that period.

Having provided this background narrative on the evolution of NSLs, I want to offer some general thoughts on the question of whether changes in the existing statutes, specifically those proposed in H.R. 3189, are appropriate. My understanding is that the goal of H.R 3189 encompasses both addressing the problems identified in the Inspector General Reports and generally enhancing the privacy protections integrated into the statutes. I think that this legislation, and other proposals like it, offer an opportunity to open a much broader discussion about the legal status of non-content transactional information and the manner in which it should be protected. I have four general comments on the proposed legislation.

First, I believe the legal standard for NSLs should remain that of relevance to an authorized investigation and not, as H.R. 3189 provides, be returned to the pre-Patriot Act standard of "specific and articulable facts." Based on my own experience with FBI national security operations, I am convinced that counter-terrorism operations are qualitatively different from the traditional counterintelligence operations for which the "specific and articulable facts" standard was originally crafted. Further, I believe this distinction has become even more pronounced since 9/11, given the imperative for the FBI to take a more preventative approach to counter-terrorism and recent revision of the Attorney General guidelines that govern those investigations. These changes actually increase the probability that FBI agents will be required to assess threat information in environments where the quality of available information falls far short of "specific." FBI counter-terrorism operations will suffer if the FBI cannot expeditiously obtain relevant information in these settings and I think that the need for the harmonization of criminal and national security legal standards for the acquisition of transactional information remains as vital now as it was at the time of the Patriot Act. Furthermore, I think that vast majority of the problems noted in the IG reports flow more from the delegation of signature authority to the field office level than from the change in the legal standard.

Second, I think that any increase in privacy risks posed by the continued use of the relevance standards are better dealt with by measures other than an across-the-board increase in the legal standard. What is needed is a much more nuanced and tailored approach that acknowledges the need for the FBI to obtain quickly all relevant counter-terrorism information (particularly that relating to threats), but also recognizes that much of the information so collected may relate to individuals of no lasting investigative interest. Such information needs to be segregated and discarded as efficiently as possible, and in a manner that inspires public confidence in its effectiveness. The FBI needs to see this task as integral to the NSL process, and not as an afterthought or a task to be accomplished when time permits. The way to achieve this result is to integrate more robust minimization and retention procedures into the NSL authorities. These mechanisms should involve, as they do in FISA, some degree of judicial review and external auditing. The provisions of H.R. 3189 that address retention provide a good starting point for movement in this direction. The sections of the resolution that address the dissemination of NSL information to law enforcement, however, would be a

thoroughly unwarranted revival of the "wall" separating intelligence and law enforcement that operated to such crippling effect prior to 9/11, and is not justified by the specific interests at stake here.

Third, I believe the current NSL statutes could be much improved if Congress would more fully outfit them. For example, many of the difficulties that recipients of NSLs have been experiencing could be alleviated if more, and more up to date, definitions were added to the statutes. In particular, the use of the undefined term "electronic communication transactional information" in the ECPA NSL seems to be at the root of many deficiencies noted by the IG. Just as Congress used the Patriot Act reauthorization legislation to clarify the enforcement and judicial review of NSLs, as well as the ability of recipients to consult legal counsel, the present situation could allow for the insertion of more complete definitions and additional clarifying language. The sections of H.R. 3189 involving the protection of privileged information are certainly a step in this direction, but I think that much more extensive and difficult works needs to be done on defining key terms.

Fourth, I think that the secrecy provisions of all the NSL statutes need to be revised in a manner that recognizes as a default position the need for secrecy, but also provides for the routine elimination of those requirements after a time certain. I believe the correct approach here is that embodied in the classification system used throughout the government. NSL information should remain subject to secrecy rules for a substantial, but finite period, which can be extended upon a specific showing of need by the FBI. I oppose the language in H.R. 3189 because I think that presumptively releasing security controls after such a short period of time is unreasonable, and has only the effect of creating a burdensome requirement for court filings in every case. An additional problem with the proposal is that it has a court making what is essentially a classification determination.

Finally, I note that comments here address the specific provisions of H.R. 3189, which presume that the acquisition of transactional information will continue to be governed by the patchwork of NSL statutes and FISA provisions. I think there is great merit in considering whether a simpler and more unified approach, such as that represented by a generic national security administrative subpoena authority for the FBI, could eliminate many of the issues noted by the Inspector General as well as provide a more effective and properly regulated investigative tool.

I hope the background information and comments that I have provided prove helpful to the Committee. I would be happy to answer any questions.

ATTACHMENT

Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215

Michael J. Woods[*]

The USA PATRIOT Act[1] has sparked intense public debate, with proponents claiming that the Act is a necessarily hard-minded response to a national crisis,[2] while opponents see unwarranted, even opportunistic, expansion of state power.[3] Perhaps no provision of the Act has generated more controversy than §215, which authorizes the FBI to seek a court order compelling the production of "any tangible things" relevant to certain counterintelligence and counterterrorism investigations.[4] Like many other provisions of the USA PATRIOT Act, §215 will expire on December 31, 2005, unless reauthorized by Congress.[5] The controversy, therefore, is likely to intensify over the coming months.

The rhetoric swirling about this provision has been extreme, despite the paucity of evidence that it has ever actually been used[6] – which suggests that the section is neither the deadly threat to civil liberties nor the vital operational

---

* The author is a former chief of the FBI's National Security Law Unit. He later served as Principal Legal Advisor to the National Counterintelligence Executive. The views expressed in this article are his own and do not necessarily reflect the position of any U.S. government component.

1. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272. The name of the Act became controversial almost immediately. *See* H.R. REP. NO. 107-236(I), at 433 (2001) (comments of Rep. Frank on the awkward and chilling effect of the name).

2. *See, e.g.*, Attorney General John Ashcroft, Prepared Remarks at the Federalist Society National Convention (Nov. 15, 2003), *available at* http://www.lifeandliberty.gov/subs/m_speeches.htm. The Justice Department Web site http://www.lifeandliberty.gov contains a collection of speeches, articles, and other materials defending the USA PATRIOT Act.

3. *See, e.g.*, Ann Beeson & Jameel Jaffer, *Unpatriotic Acts: The FBI's Power to Rifle Through Your Records and Personal Belongings Without Telling You* (American Civil Liberties Union 2003), *available at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13246&c=206. The ACLU Web site has a section, http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12126&c=207, which collects materials generally critical of the Act.

4. Pub. L. No. 107-56, §215, 115 Stat. 272, 287-288 (codified at 50 U.S.C. §§1861-1862 (Supp. II 2002)).

5. *Id.* §224, 115 Stat. 272, 295 (codified at 18 U.S.C. §2510 note (Supp. II 2002)).

6. The Attorney General announced that between the enactment of the USA PATRIOT Act on October 26, 2001, and September 18, 2003, the Justice Department had presented no applications to the Foreign Intelligence Surveillance Court for a §215 order. *See* Letter of May 19, 2004, filed by the defendant in Muslim Community Ass'n of Ann Arbor v. Ashcroft, Civil No. 03-72913 (E.D. Mich. filed July 30, 2003), *available at* http://www.aclu.org/Files/getFile.cfm?id=15842. The Department has implied, however, that §215 may have been used subsequent to September 18, 2003. *Id.*

necessity that its detractors and defenders, respectively, contend. Section 215, removed from its context in national security law, might be regarded as ominous, but placed in the larger context of operational counterintelligence authorities[7] for access to transactional information, §215 emerges as an understandable, though arguably incomplete, evolutionary step. This article is intended to supply that context, and then to examine both criticism and potential revisions of §215.

The difficulty in accomplishing this task is that, as in so many discussions of national security law, the practical relationship and functional roles of the various legal authorities are embedded in government operations that remain classified. Because few counterintelligence operational authorities have been the subject of litigation,[8] debates over these authorities tend to occur on a theoretical level, with outsiders parsing the statutory text and gleaning clues from what little exists in public records, and with insiders limiting themselves to high-level policy talk bereft of any concrete details. Since September 11, 2001, however, the FBI and the Department of Justice have declassified and released a number of key documents in response to various inquiries, investigations, and lawsuits.[9] I believe that enough information now exists in the public domain to allow an "insider" to convey a reasonably accurate picture of §215's evolution using open source material.[10]

In Section I, I will provide an overview of pre-USA PATRIOT Act authorities governing counterintelligence access to transactional information. In Section II, I will discuss the creation of §215 and address some of the principal concerns raised by critics of the USA PATRIOT Act. Finally, in Section III, I will examine potential modifications or alternatives to §215 as it currently exists.

---

7. In this article I sometimes refer to procedures for obtaining certain information as "authorities," since that term is used within the Federal Bureau of Investigation as shorthand for the statutory or regulatory authorization pursuant to which intelligence operations are conducted.

8. The one noteworthy exception concerns the Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§1801-1862 (2000 & Supp. II 2002)), which authorizes electronic surveillance and physical searches for intelligence purposes upon a showing of probable cause that the target is an agent of a foreign power. The propriety of intelligence collection under FISA is frequently litigated in espionage or terrorism prosecutions when the fruit of a FISA surveillance or search is introduced as evidence. *See, e.g.*, United States v. Squillacote, 221 F.3d 542 (4th Cir. 2000), *cert. denied*, 532 U.S. 971 (2001); United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987), *cert. denied*, 486 U.S. 1010 (1988); United States v. Badia, 827 F.2d 1458 (11th Cir. 1987), *cert. denied*, 485 U.S. 937 (1988).

9. A number of relevant documents are available in the Freedom of Information Act "electronic reading rooms" on the Justice Department Web site, http://www.usdoj.gov. Other useful collections, including materials released in the course of recent litigation, can be found on the Web sites of the American Civil Liberties Union, *at* http://www.aclu.org, the Federation of American Scientists, *at* http://www.fas.org, the Electronic Privacy Information Center, *at* http://www.epic.org, and the Center for Democracy and Technology, *at* http://www.cdt.org.

10. All the factual material in this article comes from publicly available documents, as indicated throughout. No reference to any classified material is intended.

I. AN OVERVIEW OF COUNTERINTELLIGENCE OPERATIONAL AUTHORITIES

A full understanding of §215 begins with the role of counterintelligence within the larger landscape of national security law. National security law includes a range of authorities granted to the executive branch for the defense of the nation from foreign powers. These legal authorities, subject to congressional regulation and oversight, are the basis for military operations, the collection of foreign intelligence, and covert activities.[11] "Counterintelligence" describes a subset of these activities, specifically, "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities."[12] Examples of typical counterintelligence[13] operations are the monitoring of foreign intelligence officers, the identification of possible espionage activities, the identification of international terrorist cells, and the monitoring, prevention, and disruption of terrorist activities. The distinguishing feature of a counterintelligence operation is that the target is a foreign power (state, quasi-state, or international terrorist group) or its agent;[14] targets with no tie to a foreign power are not counterintelligence targets and typically are handled through criminal investigative channels.[15]

Counterintelligence within the United States is primarily the responsibility of the FBI,[16] which conducts counterintelligence operations under guidelines

---

11. *See* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 10-31 (2001) (historical overview of this process).

12. Exec. Order No. 12,333, §3.4(a), 46 Fed. Reg. 59,941 (Dec. 4, 1981). A slight variant of this definition is codified in the National Security Act of 1947 at 50 U.S.C. §401a(3) (2000).

13. Although the term "counterintelligence" encompasses operations targeting all types of foreign powers (both traditional state powers and international terrorist groups), many documents, and the organizational structure of some agencies, distinguish between two facets of counterintelligence, namely, operations against foreign states and their intelligence services as "counterintelligence" or "foreign counterintelligence," and operations targeting international terrorist groups as "counterterrorism." In this article I use "counterintelligence" to include both types of operations.

14. "Foreign power" and "agent of a foreign power" are key terms of art in counterintelligence. Definitions of both terms may be found in FISA at 50 U.S.C. §1801(a)-(b).

15. The FBI's pre-USA PATRIOT Act investigative guidelines made this distinction clear. "Domestic terrorism" was handled under the criminal investigative guidelines. Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Domestic Security/Terrorism Investigations (March 21, 1989), *available at* http://www.usdoj.gov/ag/readingroom/generalcrimea.htm. Foreign intelligence, counterintelligence, and international terrorism were handled under the national security guidelines. Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (May 25, 1995) [hereinafter FCI Guidelines], *redacted version available at* http://www.fas.org/irp/agency/doj/fbi/terrorismintel2.pdf.

16. Exec. Order No. 12,333, *supra* note 12, at §1.14.

issued by the Attorney General.[17] Counterintelligence operations occur outside the structure of the criminal law, although they may lead to criminal prosecutions for espionage or terrorism-related crimes.

Historically, counterintelligence operations were subject to very little oversight. The revelation of abuses by the FBI, CIA, and DOD during the 1960s and 1970s, however, prompted Congress to bring counterintelligence activities under a higher degree of regulation.[18] The use of electronic surveillance in counterintelligence became subject to the Foreign Intelligence Surveillance Act of 1978 (FISA),[19] which set boundaries on use of the technique and introduced judicial supervision. The same era saw the beginning of substantial executive branch regulation of U.S. counter-intelligence and foreign intelligence activities.[20]

One legacy of this period of regulation was an enduring concern that the tools available to counterintelligence should not be used to subvert the constitutional protections of the criminal law. This concern, which had its roots in pre-FISA case law,[21] led to the creation of a "wall," built of legal and policy requirements and reinforced by culture, that separated counter-intelligence officers from criminal investigators. But the wall, prior to its partial dismantlement through the operation of the USA PATRIOT Act[22] and a subsequent court decision,[23] had the unintended consequence of depriving counterintelligence operators of some of the basic tools of criminal investigation.[24]

---

17. *See* The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (Oct. 31, 2003) [hereinafter NSI Guidelines], *redacted version available at* http://www.usdoj.gov/olp/nsiguidelines.pdf. These replace the FCI Guidelines cited *supra*, note 15.

18. The principal investigations of the abuses were conducted by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the "Church Committee") and the House Select Committee on Intelligence (the "Pike Committee"). *See* Richard A. Best, Jr., *Proposals for Intelligence Reorganization 1949-2004* (Cong. Res. Serv. RL32500) (Jul. 29, 2004), at 17-25, *available at* http://www.fas.org/irp/crs/RL32500.pdf. *See also* Banks & Bowman, *supra* note 11, at 31-35.

19. Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§1801-1862 (2000 & Supp. II 2002).

20. *See* Exec. Order No. 12,333, *supra* note 12; *see also* Exec. Order No. 11,905, 41 Fed. Reg. 7703 (Feb. 18, 1976); Exec. Order No. 12,036, 43 Fed. Reg. 3674 (Jan. 24, 1978) (both superseded by Exec. Order No. 12,333); Banks & Bowman, *supra* note 11, at 68-74.

21. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 915-916 (4th Cir. 1980) (upholding a warrantless surveillance only so long as it was conducted "primarily" for foreign intelligence reasons).

22. *See* Pub. L. No. 107-56, §§203, 218, 504, 115 Stat. 272, 278-281, 291, 364-365.

23. *In re* Sealed Case, 310 F.3d 717 (Foreign Intelligence Surveillance Court of Review 2002).

24. There are many descriptions of the history and effects of the "wall" as it existed prior to the passage of the USA PATRIOT Act. *See, e.g., id.* at 721-728; Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation, ch. 20 (May 2000), *available at* http://www.usdoj.gov/ag/readingroom/bellows20.pdf (commonly called the "Bellows Report," this document examines the FBI investigation of Dr. Wen Ho Lee; Chapter 20 contains a detailed description of the "wall"); THE 9/11 COMMISSION

FBI counterintelligence agents were authorized by FISA to conduct electronic surveillance and physical searches. However, such methods are generally used only in the end stages of an investigation, after the probable cause required for FISA surveillance is established through the use of less intrusive techniques. Indeed, FBI counterintelligence agents are under a formal requirement to use the least intrusive means first.[25] These less intrusive means include interviews, review of publicly available information, surveillance in areas where no reasonable expectation of privacy exists, consensual monitoring, "mail covers," and the use of undercover operatives.[26] They also include the use of "national security letters" to obtain information for counterintelligence purposes.[27]

Congress approved the use of national security letters in response to the need for counterintelligence agents to obtain transactional information about investigative subjects. "Transactional" information broadly describes information that documents financial or communications transactions without necessarily revealing the substance of those transactions. Telephone billing records that list the numbers dialed by a particular subscriber, records from an Internet service provider showing when a user logged onto an account or to whom the user sent email, records of bank accounts or transfers of money between financial institutions, and credit records are all examples of transactional information.

Transactional information has developed into an extraordinarily valuable source of data for counterintelligence analysts, particularly in their efforts to identify international terrorists. Terrorists can limit their exposure to the interception of the content of communications by using counter-surveillance techniques that run the gamut from the ancient (human couriers, secret writing, simple word codes) to the modern (computer-based encryption and steganography).[28] It is far more difficult for them to cover their transactional

---

REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 78-80, 270-271 (2004).

25. *See* Exec. Order No. 12,333, *supra* note 12, at §2.4; NSI Guidelines, *supra* note 17, at 7.

26. The actual descriptions of investigative techniques remain classified, but their inclusion in the NSI Guidelines can be inferred from definitions found in unclassified portions of the document. *See* NSI Guidelines, *supra* note 17, at 33-38. A "mail cover" is an investigative technique in which the FBI obtains copies of the outside surfaces of mail delivered through U.S. postal channels.

27. National security letters are described *infra* in the text accompanying notes 45-85.

28. "Steganography" refers to the practice of concealing messages within innocuous documents, images, or other media. The frequency with which computer-based encryption and steganography are actually used by terrorists has been debated since before the September 11 attacks, but indications of such use regularly emerge in public reports. *See, e.g., The Terrorist Threat Confronting the United States: Hearing Before the Senate Select Committee on Intelligence*, 107th Cong. (2002) (testimony of Dale L. Watson, FBI Exec. Asst. Director), *available at* http://www.fbi.gov/congress/congress02/watson020602.htm (FBI view on use of encryption by terrorists); Nick Fielding, *Al-Qaeda Betrayed by its Simple Faith in High-Tech*, THE TIMES (London), Aug. 8, 2004, at 14; Ariana Eunjung Cha & Jonathan Krim, *Terrorists'*

footsteps. Therefore, counterintelligence analysts seek to use information about financial, credit, and communications transactions to construct link diagrams of terrorist networks.[29] A good example of this technique is the extensive, and tragically retrospective, link analysis of the nineteen September 11 hijackers.[30]

The legal status of transactional information has evolved dramatically since the mid-1970s, following public awareness that nearly all transactional information resides beyond the protections of the Fourth Amendment. In *United States v. Miller*, the Supreme Court held that the government can use a grand jury subpoena to obtain a defendant's financial records from a bank without intruding into an area protected by the Fourth Amendment.[31] The Court pointed out that "'no interest legitimately protected by the Fourth Amendment' is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into 'the security a man relies upon when he places himself or his property within a constitutionally protected area.'"[32] The checks, deposit slips, and bank statements produced in response to the subpoena were not the defendant's "private papers," the Court held; rather, they contained "only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[33] By handing over this information to a third party, the defendant took the risk that it would be conveyed to the government by that third party.[34] Finally, the Court noted that the lack of notice to the defendant that the government had obtained his information did not infringe upon a protected interest.[35]

To be sure, expectations of privacy may have changed in the three decades since *Miller* was decided. Commercial enterprises and financial institutions today commonly allow customers to state a preference about how their personal information will be used, and they often market guarantees of

---

Online Methods Elusive, WASH. POST, Sept. 19, 2001, at A14; Declan McCullagh, *Bin Laden: Steganography Master?*, WIRED NEWS, Feb. 7, 2001, *available at* http://www.wired.com/news/politics/0,1283,41658,00.html. *See generally* Allan Cullison, *Inside Al-Qaeda's Hard Drive*, ATLANTIC MONTHLY, Sept. 2004, at 55-72.

29. This analytical process can range from simple "link analysis" to far more ambitious "data mining." These techniques and the legal environment relevant to the underlying transactional information attained some notoriety when featured in the Defense Department's "Total Information Awareness" program. *See* Gina Marie Stevens, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws* (Cong. Res. Serv. RL31730) (2003), *available at* http://www.fas.org/irp/crs/RL31730.pdf; Mary DeRosa, *Data Mining and Data Analysis for Counterterrorism* (Center for Strategic and International Studies) (2004), *available at* http://www.cdt.org/security/usapatriot/20040300csis.pdf.

30. *See* THE 9/11 COMMISSION REPORT, *supra* note 24, at 215-253.

31. United States v. Miller, 425 U.S. 435 (1976).

32. *Id.* at 440, *citing* Hoffa v. United States, 385 U.S. 293, 301-302 (1966).

33. 425 U.S. at 440, 442.

34. *Id.* at 443.

35. *Id.* at 443 n.5; *see also* Securities and Exchange Comm'n v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984).

privacy. From this, a customer now could reasonably conclude that he or she retained control over data entrusted to these third parties. In spite of criticism that it needs re-examination in light of these and other technological developments,[36] however, *Miller* remains the law for now.

The *Miller* decision prompted Congress in 1978 to enact the Right to Financial Privacy Act (RFPA).[37] In broad terms, the RFPA created statutory protection for the records that the *Miller* Court found were beyond the reach of the Fourth Amendment. The Act defined the scope of the records protected and generally required that notice be given to account holders when records were disclosed in response to legitimate government inquiries.[38] The statute aimed to "strike a balance between customers' right of privacy and the need of law enforcement agencies to obtain financial records pursuant to legitimate investigations."[39] Congress included an exception for foreign intelligence investigations, allowing requests for protected information by government authorities who were "authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities" to be honored without notice to the targeted customers.[40] Writing just two years after the Church and Pike Committees had completed their work, however, Congress remained wary of counterintelligence, and it noted that the exception should "be used only for legitimate foreign intelligence investigations; investigations proceeding only under the rubric of 'national security' do not qualify."[41]

By the mid-1980s, the FBI had begun to push for authority to compel the production of financial records in counterintelligence matters without a judicial order. The existing RFPA language allowed the FBI (and other counterintelligence agencies) to make requests for information, but it did not require financial institutions to comply. The FBI argued that while most such

---

36. *See, e.g., Anti-Terrorism Investigations and the Fourth Amendment After September 11: Where and When Can the Government Go to Prevent Terrorist Attacks?, Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 108th Cong. (2003) (statement of James X. Dempsey, Exec. Director, Center for Democracy and Technology), *available at* http://www.house.gov/judiciary/dempsey052003.pdf.

37. Right to Financial Privacy Act of 1978, Title XI of the Financial Institutions Regulatory and Interest Rates Control Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (codified as amended at 12 U.S.C.A. §§3401-3422 (West 2001 & Supp. 2004)). *See O'Brien*, 467 U.S. at 745. *See also* H.R. REP. NO. 95-1383, at 34 (1978), *reprinted in* 1978 U.S.C.C.A.N. 9273, 9306.

38. The RFPA contained a general prohibition on government access to protected records, *see* Pub. L. No. 95-630, §1102, 92 Stat. 3697, 3697-3698, although it defined exceptions to the prohibition for subpoenas, search warrants, and formal requests. *Id.* §§1102, 1105-1108, 92 Stat. 3697, 3697-3702. Use of these exceptions required notice to the customer, although that notice could be delayed in certain circumstances. *Id.* §§1105-1109, 1112, 1113, 92 Stat. 3697, 3699-3703, 3705-3707.

39. *See* H.R. REP. NO. 95-1383, at 33.

40. Pub. L. No. 95-630, §1114(a)(1)(A), 92 Stat. 3697, 3707; *see* H.R. REP. NO. 95-1383, at 55.

41. H.R. REP. NO. 95-1383, at 55.

institutions did comply, in "certain significant instances" they did not, often citing the constraints of state constitutions or banking privacy laws.[42] The congressional response[43] was to give the FBI[44] specific authority to compel the production of financial records using a "national security letter."[45]

With the introduction of compulsory process, Congress also created safeguards to govern the FBI's use of that authority. The statute required that a high-ranking FBI official certify: (1) that the information is sought "for foreign counterintelligence purposes," and (2) that "there are specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978."[46] The new provision, like the original RFPA, however, both failed to require notification of the target and affirmatively prohibited the financial institution from disclosing the existence of the national security letter to anyone.[47] The House Permanent Select Committee on Intelligence found that the "FBI could not effectively monitor and counter the clandestine activities of hostile espionage agents and terrorists if they had to be notified that the FBI sought their financial records for a counterintelligence investigation."[48] Nevertheless, the legislators expressed a preference that the Director of the FBI restrict the delegation of national security letter authority and that the requirements for handling information obtained through the RFPA be integrated into the Attorney General's guidelines for FBI counterintelligence.[49]

Congress seemed far more receptive to the idea of FBI counterintelligence access to financial records in 1986 than it did in 1978. In part that could reflect a greater confidence in the regulation of counterintelligence activities. Executive Order 12,333[50] was by that time firmly established as the basis for jurisdiction and operational rules within the U.S. intelligence community. Pursuant to that order, the FBI was operating under Attorney General guidelines that governed all counterintelligence activity and that set standards

---

42. *See* H.R. REP. NO. 99-690(I), at 15-16 (1986), *reprinted in* 1986 U.S.C.C.A.N. 5327, 5341-5342.

43. Intelligence Authorization Act for Fiscal Year 1987, Pub. L. No. 99-569, §404, 100 Stat. 3190, 3197 (1986) (codified at 12 U.S.C. §3414(a)(5)(A)-(D) (2000 & Supp. II 2002)).

44. Only the FBI has *compulsory* authority, although the request provision in 12 U.S.C. §3414(a)(1)(A) remains available to other agencies. The request provision is used, for example, by counterintelligence components within the Department of Defense. *See* Department of Defense Dir. No. 5400.12, *Obtaining Information from Financial Institutions* (Feb. 6, 1980), at encl. 5, *available at* http://www.dtic.mil/whs/directives/corres/html/540012.htm.

45. The term "national security letter" does not appear in the statute, but the legislative history indicates that it was in common use by that time. *See* H.R. REP. NO. 99-690(I), at 15.

46. Pub. L. No. 99-569, §404.

47. *Id.*

48. H.R. REP. NO. 99-690(I), at 15.

49. *See id.* at 17; H.R. CONF. REP. NO. 99-690 (III), at 24, *reprinted in* 1986 U.S.C.C.A.N. 5371, 5384. This language was integrated into the guidelines. *See* FCI Guidelines, *supra* note 15, at 29-30.

50. Exec. Order No. 12,333, *supra* note 12, at §3.4(a).

and approval authority for the various facets of counterintelligence investigations.[51] The 1986 legislation may also reflect a change in attitude about the need for counterintelligence. The early 1980s saw a dramatic increase in espionage cases, and interest in counterintelligence rose accordingly.[52] Moreover, Congress began to see international terrorism as a serious national security threat.[53]

In granting compulsory process to FBI counterintelligence in 1986, Congress created a new, hybrid legal standard: "specific and articulable facts giving reason to believe" that the targeted person is an "agent of a foreign power."[54] The "agent of a foreign power" criterion was not new; it had been established in the Foreign Intelligence Surveillance Act of 1978 as a way to identify proper subjects of counterintelligence electronic surveillance.[55] The

---

51. *See* FCI Guidelines, *supra* note 15.

52. The media dubbed 1985 the "Year of the Spy" after some fifteen people (including Jonathan Pollard, Larry Wu-Tai Chin, Edward Lee Howard, and the members of the Walker spy ring) were arrested for espionage that year. *See* Defense Personnel Security Research Center, *Recent Espionage Cases: 1975-1999* (Oct. 1999), *available at* http://www.dss.mil/training/espionage/.

53. *See, e.g.*, H.R. REP. NO. 99-690(1), at 14-17. The analogous discussion in 1978 contained no mention of terrorism and referred only to the "intelligence operations of foreign governments." *See* H.R. REP. NO. 95-1383, at 55.

54. Pub. L. No. 99-569, §404.

55. FISA authorizes electronic surveillance (and, since 1994, physical searches) of foreign powers and their agents when the government demonstrates, *inter alia*, probable cause that the targets meet the relevant definitions. *See generally* 50 U.S.C. §§1801-1829. FISA defines "agent of a foreign power" as:

> (1) any person other than a United States person, who –
> (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
> (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or
>
> (2) any person who –
> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to

innovation was in the quantum of proof required: "specific and articulable facts giving reason to believe." The Conference Report noted that the standard was "significantly less stringent than the requirement of 'probable cause,'" and it indicated that the "reason to believe" standard should "take into account the facts and circumstances that a prudent investigator would consider insofar as they provide an objective, factual basis for the determination."[56] An earlier report indicated that the House considered the higher standard of "probable cause" inappropriate, given the holding in *Miller*.[57]

Shortly before Congress modified the RFPA to provide national security letter authority, it enacted the Electronic Communications Privacy Act (ECPA).[58] ECPA broadly updated the law governing electronic communications by refining prohibitions on their interception, extending legal protections for traditional telephone service to include all wire and electronic communications services, and regulating stored wire and electronic communications.[59]

In many respects, ECPA was an attempt to keep pace with evolving technology. It represented the first significant legislation to address what would become the Internet.[60] In particular, ECPA was concerned with the invasive potential of advancing technology. The Senate report opened by quoting the prescient dissent in *Olmstead v. United States*: "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[61] The report continued by observing that the growing use of computers enabled the proliferation of personal information stored in areas beyond the control of the individual. Citing *Miller*, the report concluded that, absent statutory protection, such information "may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties."[62]

ECPA addressed this problem by extending statutory protection to electronic and wire communications stored by third parties (for example, on the servers of an Internet service provider or corporate network) and to

---

engage in activities described in subparagraph (A), (B), or (C).

50 U.S.C. §1801(b).

56. H.R. CONF. REP. NO. 99-952, at 23 (1986).

57. H.R. REP. NO. 99-690(I), at 17.

58. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C.A. §§2701-2712 (West 2000 & Supp. 2004)).

59. *See* S. REP. NO. 99-541, at 1-3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-3556.

60. *See id.*

61. *Id.* at 2, *quoting* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

62. S. REP. NO. 99-541, at 3.

electronic communication transactional records.[63] The Act also restricted the government's access to live telephone transactional data (commonly known as "pen register" and "trap and trace" data), requiring it to obtain a court order based upon a certification of relevance to an ongoing criminal investigation.[64]

Like the RFPA, ECPA contained a special provision for counter-intelligence access. Section 201 of ECPA allowed the FBI to compel the production of "subscriber information and toll billing records information, or electronic communication transactional records" from a "wire or electronic communications service provider."[65] The issuance of a national security letter under this provision required the certification of a high-ranking FBI official[66] that the information sought was relevant to a foreign counterintelligence investigation and that there were "specific and articulable facts giving reason to believe" that the target was a foreign power or agent of a foreign power under the FISA definitions.[67] The ECPA provision thus mirrored the standard in the 1986 amendment to the RFPA.

ECPA's drafters also aimed for a "carefully balanced provision" that addressed operational necessities.[68] The "specific and articulable facts" standard emerged as an appropriate balance for counterintelligence access: criminal investigators could obtain information upon a certification of relevance (but generally with notice to the target), while counterintelligence investigators could obtain the information in secret,[69] but only after meeting

---

63. Pub. L. No. 99-508, Title II, 100 Stat. 1848, 1860-1868 (codified as amended at 18 U.S.C.A. §§2701-2709, 2711 (West 2000 & Supp. 2004)).

64. Pub. L. No. 99-508, §§301-302, 100 Stat. 1848, 1868-1872 (codified as amended at 18 U.S.C. §§3121-3127 (2000 & Supp. II 2002)). A pen register is a device that records the numbers that a target telephone is dialing. A trap and trace device captures the telephone numbers that dial a target telephone. *See* 18 U.S.C. §3127. The USA PATRIOT Act provides that this authority also applies to Internet accounts and other computer-based communications. *See* Pub. L. No. 107-56, §216(c), *amending* 18 U.S.C. §3127.

65. Pub. L. No. 99-508, §201, 100 Stat. 1848, 1867 (codified as amended at 18 U.S.C. §2709).

66. Though not explicit in the statute, the legislative history indicates that signature authority should be limited in the FBI to Deputy Assistant Directors and above. *See* S. REP. NO. 99-541, at 44.

67. Pub. L. No. 99-508, §201, 100 Stat. 1848, 1867 (codified as amended at 18 U.S.C. §2709).

68. The Senate report provides in part:

> Section 2709 is a carefully balanced provision that remedies the defect in current law that the FBI cannot gain access on a mandatory basis to telephone toll records maintained by communications common carriers, for counterintelligence purposes. As a result, especially in states where public regulatory bodies have created obstacles to providing such access, the FBI has been prevented from obtaining these records, which are highly important to the investigation of counterintelligence cases.

S. REP. NO. 99-541, at 44.

69. Like the RFPA, ECPA prohibited the recipients of a national security letter from disclosing its existence. Pub. L. No. 99-508, §201, 100 Stat. 1848, 1867 (codified at 18 U.S.C. §2709(c)). [Author's note: After this article was written, a district court held §2709 unconstitutional based on its interpretation of the secrecy provision in §2709(c). *See* Doe v. Ashcroft, 2004 WL 2185571 (S.D.N.Y. Sep. 28, 2004), *available at* http://www.nysd.uscourts.

the more stringent standard. The standard was viewed as consistent with the investigative standards imposed on FBI counterintelligence by the Attorney General guidelines.[70]

The counterintelligence provision of ECPA was amended twice prior to the passage of the USA PATRIOT Act. It originally gave the FBI access to subscriber information, toll billing records, and electronic communications transactional records of anyone who met the FISA definition of a foreign power or agent of a foreign power (to the "specific and articulable facts" standard).[71] The FBI subsequently sought authority to obtain subscriber information in order to identify (or to confirm the identity of) people who contacted or were in contact with agents of a foreign power.[72] The FBI offered three operational examples: (1) persons whose phone numbers were listed in an address book seized from a suspected terrorist; (2) persons who called a foreign embassy and asked to speak to an intelligence officer; and (3) callers to the home of a suspected intelligence officer or terrorist.[73] In each case, the FBI's use of ECPA's counterintelligence provision or other authorities against a foreign intelligence officer or terrorist target would yield the phone number of the caller, but the FBI could not obtain subscriber information about that caller. A 1993 amendment to ECPA gave the FBI the authority it sought, with some limitations.[74] Congress amended the provision again in 1997, expressly

---

gov/rulings/04CV2614_Opinion_092904.pdf. The court found that §2709 lacks sufficient procedural protections, given the nature of the information subject to its compulsory process. *See id.* at 45-82. After extensive discussion, the court also concluded that the §2709(c) secrecy provision violates the First Amendment, because it is not narrowly tailored to serve the government's compelling interests. *See id.* at 83-116. The decision, if upheld in its entirety, will merit extensive analysis. Given its timing, however, and the unknown outcome of the pending appeal, I merely cite *Doe* briefly here and in other footnotes where it would most affect arguments in the text.]

70. The portions of the Attorney General guidelines setting out the standards for opening the various forms of counterintelligence investigations remain classified. ECPA's legislative history notes cryptically that "the Senate Select Committee on Intelligence has informed the Judiciary Committee that the language contained in the bill would not significantly alter the application of the current FBI investigative standard in this area." S. REP. NO. 99-541, at 45.

71. Pub. L. No. 99-508, §201, 100 Stat. 1848, 1867. "Subscriber information" in the 1986 version was replaced with "name, address, and length of service" in a 1993 amendment. *Compare* Pub. L. No. 99-508, §201 *with* Pub. L. No. 103-142, §§1-2, 107 Stat. 1491, 1491-1492 (1993).

72. H.R. REP. NO. 103-46, at 2 (1993), *reprinted in* 1993 U.S.C.C.A.N. 1913, 1914.

73. *Id.* at 3.

74. The new language gave the FBI access to subscriber information on anyone who was in contact with a terrorist, but it limited that access to situations in which circumstances "gave reason to believe that the communication concerned" terrorism or clandestine intelligence activities. *See* Act of Nov. 17, 1993, Pub. L. No. 103-142, §2, 107 Stat. 1491, 1492 (1993). This distinction was meant to clarify that the authority not be used to target innocent contacts with agents of foreign powers, such as routine calls to foreign embassy staff about visas or other general information matters. *See* H.R. REP. NO. 103-46, at 2-3.

defining the phrase "toll billing records" to mean "local and long distance toll billing records."[75]

The final type of national security letter emerged in 1995, when the FBI sought counterintelligence access to credit records.[76] The FBI stated that RFPA national security letters had proven very useful, but that counter-intelligence agents still had to employ intrusive or time-consuming techniques (physical and electronic surveillance, mail covers, and canvassing of local banks) simply to determine where targeted individuals maintained accounts.[77] The same information was readily available from credit bureaus ("consumer reporting agencies") and was commonly obtained in criminal investigations through the use of a subpoena.[78] Congress's response was to amend the Fair Credit Reporting Act (FCRA)[79] by giving the FBI national security letter authority to obtain certain information from credit reporting agencies.[80] The authority essentially replicated that granted in the 1993 ECPA amendment, employing the same legal standard: "necessary for the conduct of an authorized foreign counterintelligence investigation" and "specific and articulable facts" giving reason to believe the target was (or was in contact with) an agent of a foreign power.[81] Similarly, the new FCRA provision embodied two levels of access to information: if the target was an agent of a foreign power, the FBI could get the identity of all financial institutions at which the target maintained an account; if the target was merely in contact with an agent of a foreign power, the FBI got "identifying information" limited to "name, address, former addresses, places of employment, or former places of employment."[82]

The one departure from the RFPA and ECPA models was in the area of disclosure. The FCRA language prohibits disclosure of the national security letter by employees of the credit reporting agency "other than [to] those officers, employees, or agents of a consumer reporting agency necessary to fulfill the requirement to disclose information" to the FBI.[83] This language was intended to clarify what is apparently assumed in the other statutes, namely, that employees may disclose the existence of the national security

---

75. Intelligence Authorization Act for Fiscal Year 1997, Pub. L. No. 104-293, §601(a), 110 Stat. 3461, 3469 (1996); *see* S. REP. NO. 104-258, at 22-23 (1996), *reprinted in* 1997 U.S.C.C.A.N. 3945, 3967-3968.

76. *See* H.R. CONF. REP. NO. 104-427, at 34-36 (1995), *reprinted in* 1995 U.S.C.C.A.N. 983, 996-998.

77. *See id.* at 36.

78. *See id.* at 35-36.

79. Pub. L. No. 91-508, Title VI, 82 Stat. 1127 (1970).

80. Intelligence Authorization Act for Fiscal Year 1996, Pub. L. No. 104-93, §601(a), 109 Stat. 961, 974-977 (1996) (codified as amended at 15 U.S.C. §1681u (2000 & Supp. II 2002)).

81. Pub. L. No. 104-93, §601(a), 109 Stat. 961, 975.

82. *Id.*

83. *Id.* The ECPA and RFPA provisions prohibit disclosure to "any person." 18 U.S.C. §2709(c) (ECPA); 12 U.S.C. §3414(a)(5)(D) (RFPA).

letter in compliance with the credit bureau's internal policies.[84] Presumably, this language would permit disclosure to relevant managers or the consumer reporting agency's legal counsel. Finally, the FCRA amendment gave the FBI access to a consumer's full credit report, but only if a court found that the FBI's information met the same legal standard – "specific and articulable facts" – as in the other section of the amendment.[85]

In addition to the national security letter authorities just described, in a 1998 amendment to the Foreign Intelligence Surveillance Act the FBI acquired two new tools to collect transactional information.[86] The amendment for the first time permitted "pen register" and "trap and trace" authorization to be obtained through the FISA process.[87] This change addressed a longstanding anomaly in the counterintelligence environment: unlike criminal investigators who could use Title 18 authority to install pen registers and trap and trace devices,[88] counterintelligence agents could not prospectively collect telephone transactional information on suspected spies or terrorists.[89] The new FISA pen register and trap and trace authority mirrored the criminal investigative authority that had existed since 1986.[90] Unlike the criminal statute, however, the standard for a FISA pen register or trap and trace order was not "relevance" to an ongoing investigation. Rather, it was set at something like the hybrid standard for national security letters: "relevance" plus "information which demonstrates that there is reason to believe" that the targeted telephone line "has been or is about to be used in communication with" a person engaged in international terrorism, a person engaged in clandestine intelligence activities, or any foreign power or agent of a foreign power under circumstances indicating clandestine intelligence or terrorist

---

84. *See* H.R. CONF. REP. NO. 104-427, at 39; *see also* Doe v. Ashcroft, *supra* note 69, at 51-55 (comparing non-disclosure language in FCRA to that in ECPA).

85. Pub. L. No. 104-93, §601(a). The provision was largely useless prior to the USA PATRIOT Act, since FBI counterintelligence agents did not have ready access to a court that could issue such an order. The Foreign Intelligence Surveillance Court likely had no jurisdiction to entertain a request under this section. *See* 50 U.S.C. §§1803(a), 1822(c) (defining jurisdiction of the court). Recourse to a federal district court would have involved interaction with prosecutors, and thus triggered elaborate "wall" restrictions meant to keep counterintelligence agents and prosecutors at arm's length. *See supra* note 24. Obtaining a simple credit report typically would not have justified the efforts and risks associated with those restrictions.

86. *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, Title VI, 112 Stat. 2396, 2404-2413 (1998).

87. *Id.* at §601, 112 Stat. 2396, 2404-2410.

88. *See* 18 U.S.C. §§3121-3127.

89. Counterintelligence agents could, however, collect historical transactional data using the ECPA national security letter authority. *See* 18 U.S.C.§2709.

90. *See generally* Pub. L. No. 105-272, at §601, 112 Stat. 2396, 2404-2410. The analogous criminal law authority is codified at 18 U.S.C. §§3121-3127 and authorizes the use of pen registers and trap and trace devices upon a government certification that the information likely to be obtained is relevant to an ongoing criminal investigation. *Id.* at §3123(a).

activities.[91] The FISA amendment also created procedures for emergency use of the authority, certain restrictions on the use of information obtained through the authority, and a notification and challenge procedure triggered when information obtained is used in a subsequent proceeding.[92] The notification and challenge procedure mirrors those found elsewhere in FISA for electronic surveillance and physical searches.[93]

The 1998 amendment to FISA also created the direct antecedent of §215 of the USA PATRIOT Act. It allowed the FBI to seek a FISA court order compelling the production of business records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.[94] The standard was set at the now-familiar "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or agent of a foreign power."[95] Like the new pen register authority and all of the existing national security letter authorities, this provision imposed a non-disclosure requirement on the recipients of the court order.[96] In stating the duties of the Foreign Intelligence Surveillance Court judge, it simply replicated the language of the pen register and trap and trace provision: "Upon application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified . . . if the judge finds that the application satisfies the requirements of this section."[97]

There is almost no legislative history for these two new provisions. They emerged in the Senate version of the Intelligence Authorization Act for Fiscal Year 1999, but they are not otherwise mentioned in the conference report or floor debate.[98] The congressional debate and the press tended to focus on another section, which amended the criminal electronic surveillance law (commonly called "Title III") to facilitate "roving" surveillance.[99] It is reasonable to assume that, as in prior instances, the FBI argued that it needed authority to compel production of materials not then accessible through the use of national security letters. Since counterintelligence agents were

---

91. Pub. L. No. 105-272, §601, 112 Stat. 2396, 2405-2406 (codified as amended at 50 U.S.C. §1842(c)). With only slight variations, this new authority adopted the standard for ECPA national security letters established in 18 U.S.C. §2709.

92. Pub. L. No. 105-272, §601, 112 Stat. 2396, 2407-2410 (codified as amended at 50 U.S.C. §§1843-1845).

93. *See* 50 U.S.C. §§1806, 1825.

94. Pub. L. No. 105-272, §602, 112 Stat. 2396, 2410-2412.

95. *Id.*

96. *Id.* The non-disclosure provision incorporated the clarifying language ("other than those officers, agents or employees . . . necessary to fulfill the requirement") developed for the FCRA national security letter. *Id.*; *see supra* text accompanying notes 83-84.

97. Pub. L. No. 105-272, §602, 112 Stat. 2396, 2411.

98. *See* H.R. CONF. REP. NO. 105-780 (1998), at 32.

99. Pub. L. No. 105-272, §604, 112 Stat. 2396, 2413; *see, e.g.*, Vernon Loeb, *Anti-Terrorism Powers Grow, "Roving" Wiretaps, Secret Court Orders Used to Hunt Suspects*, WASH. POST, Jan. 29, 1999, at A23. The fact that the change to Title III (a criminal authority) occurred via the intelligence authorization act was particularly controversial and dominated the public debate.

"walled" off from the use of criminal authorities like grand jury subpoenas, a records custodian could effectively stall a counterintelligence investigation by refusing to release records absent compulsory process.[100] Such a refusal could have been motivated by a concern over the effect of state laws or civil liability, or it could have been an act of civil disobedience or simple unwillingness to cooperate.[101]

In summary, on the eve of the September 11 terrorist attacks the FBI had five separate legal authorities that addressed the need to compel production of transactional information in counterintelligence investigations: three types of national security letters (under RFPA, ECPA, and FCRA),[102] the FISA pen register/trap and trace authority, and the FISA business records authority. All of these authorities specified the types of records that could be obtained, and all the records specified were, according to the reasoning of the Supreme Court in *Miller*, outside the protection of the Fourth Amendment. All of the authorities required, in essence, that the information sought be relevant to an authorized counterintelligence investigation and that the FBI demonstrate "specific and articulable facts giving reason to believe" that the investigative targets were foreign powers or agents thereof.

II. THE USA PATRIOT ACT AND SECTION 215

Much has already been written about the creation of the USA PATRIOT Act in the chaotic weeks following September 11, 2001.[103] The Bush

---

100. There is some hint of this argument in an FBI document released subsequent to passage of the USA PATRIOT Act. In it, speaking of USA PATRIOT Act §215 but possibly referring to the background of the 1998 FISA amendment as well, the FBI Office of the General Counsel wrote:

> In the past, the FBI has encountered situations in which the holders of relevant records refused to produce them absent a subpoena or other compelling authority. When those records did not fit within the defined categories for National Security Letters or the four categories then defined in the FISA business records section, the FBI had no means of compelling production.

Communication from the FBI Office of the General Counsel to All Divisions, New Legislation, Revisions to FCI/IT Legal Authorities, Foreign Intelligence Surveillance Act (Oct. 26, 2001), *attached to* Letter from Assistant Attorney General Bryant to Senator Feingold (Dec. 23, 2002), *available at* http://fas.org/irp/agency/doj/fisa/doj-fisa-patriot-122302c.pdf.

101. *See supra* notes 42, 68.

102. Occasionally, a separate Title 50 authority granted to counterintelligence and security investigators also is referred to as "national security letter" authority. *See* 50 U.S.C. §436. However, it is beyond the scope of this discussion, because the authority is consent-based, and it applies only to executive branch employees who hold, or are seeking, a security clearance. *Id.*

103. The Act inspired a flood of notes, commentary, and symposia in the legal community. *See, e.g.*, Rebecca A. Copeland, *War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America*, 35 TEX. TECH L. REV. 1 (2004); Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U.L. REV. 607 (2003); Panel Discussion, *The USA-PATRIOT Act and the American Response to Terror: Can We Protect Civil Liberties After*

administration began developing a legislative proposal within days after the attacks.[104] Congress acted with great speed: the House version of the Act was introduced on October 2 and passed ten days later;[105] the Senate version was introduced on October 4 and passed in just seven days.[106] The final version of the Act was introduced on October 23, 2001, and was signed into law on October 26, 2001.[107] The end product is massive, running to 130 printed pages.[108]

A very considerable portion of the Act is devoted to changes in criminal, immigration, and money laundering statutes.[109] Within the sections that affect counterintelligence authorities, the revisions to national security letter and related authorities are generally overshadowed by enhancements to the FISA search and surveillance provisions and new rules for information sharing.

The USA PATRIOT Act revisions to authorities governing counter-intelligence access to transactional information are spread across three sections: §214 ("Pen register and trap and trace authority under FISA"), §215 ("Access to records and other items under the Foreign Intelligence Surveillance Act"), and §505 ("Miscellaneous national security authorities"). The cumulative effect of these three sections is to make an across-the-board adjustment of the legal standard for access from "relevance" plus "specific and articulable facts giving reason to believe" the target was a foreign power or an agent of one, to simple "relevance" to an investigation to protect against international terrorism or clandestine intelligence activities (provided such an investigation of a U.S. person is not based solely on protected First

---

September 11?, 39 AM. CRIM. L. REV. 1501 (2002); Symposium, *First Monday Civil Liberties in a Post-9/11 World*, 27 SETON HALL LEGIS. J. 1 (2002); Alison A. Bradley, Comment, *Extremism in the Defense of Liberty? The Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT Act*, 77 TUL. L. REV. 465 (2002); Jennifer C. Evans, Comment, *Hijacking Civil Liberties: The USA PATRIOT Act of 2001*, 33 LOY. U. CHI. L.J. 933 (2002); Nathan C. Henderson, Note, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications*, 52 DUKE L.J. 179 (2002); Jacob R. Lilly, Note, *National Security at What Price?: A Look into Civil Liberty Concerns in the Information Age Under the USA PATRIOT Act of 2001 and a Proposed Constitutional Test for Future Legislation*, 12 CORNELL J.L. & PUB. POL'Y 447 (2003); Stephen D. Lobaugh, Note, *Congress' Response to September 11: Liberty's Protector*, 1 GEO. J. L. & PUB. POL'Y 131 (2002); Sharon H. Rackow, Comment, *How the USA PATRIOT Act Will Permit Governmental Infringement Upon the Privacy of Americans in the Name of "Intelligence" Investigations*, 150 U. PA. L. REV. 1651 (2002); Jeremy C. Smith, Comment, *The USA PATRIOT Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security*, 82 N.C. L. REV. 412 (2003).

104. *See* 147 CONG. REC. S10,991 (2001) (comments of Sen. Leahy on timing of legislation); 147 CONG. REC. S11,020-S11,021 (2001) (comments of Sen. Feingold on truncated legislative process).

105. H.R. 2975, 107th Cong. (2001).

106. S. 1510, 107th Cong. (2001).

107. H.R. 3162, 107th Cong., *enacted as* Pub. L. No. 107-56, 115 Stat. 272 (2001).

108. *See id.*, 115 Stat. 272-402.

109. *See id.*

Amendment activity).[110] Section 505 also lowers the signature authority for the three types of FBI national security letters from Deputy Assistant Director to Special Agent in Charge.[111] The apparent intent of Congress here was to make the legal standard for basic counterintelligence investigations analogous to that for the corresponding criminal investigations, a change viewed as appropriate in light of the evolving terrorist threat.[112] In a different section, the Act creates a broad new investigative authority by inserting language in the FCRA that compels consumer reporting agencies to furnish

> a consumer report of a consumer and all other information in a consumer's file to a government agency authorized to conduct investigations of, intelligence or counterintelligence activities or analysis related to, international terrorism when presented with a

---

110. The wording of the new standard varies slightly depending on which statute is being amended. The FISA pen register/trap and trace provision requires a certification that "the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing 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." Pub. L. No. 107-56, §214(a)(2), 115 Stat. 272, 286 (codified at 50 U.S.C. §1842(c)(2)). The new ECPA language requires that the records sought 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." Pub. L. No. 107-56, §505(a), 115 Stat. 272, 365 (codified at 18 U.S.C. §2709(b)(1)-(2)). The new RFPA language requires that the information be "sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States." Pub. L. No. 107-56, §505(b), 115 Stat. 272, 365-366 (codified at 12 U.S.C. §3414(a)(5)(A)). The new FCRA language requires a certification that the information is "sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States." Pub. L. No. 107-56, §505(c), 115 Stat. 272, 366 (codified at 15 U.S.C. §1681u(a)-(c)).

111. Prior to 2001, only about ten FBI officials (mostly located in Washington, D.C.) were authorized to sign national security letters. This meant that agents seeking to use a letter had to submit the request and supporting materials through a long chain of approvals. Section 505 authorized "Special Agents in Charge," that is, heads of the FBI's fifty-six field offices, to sign national security letters. The change makes national security letters far more accessible to counterintelligence agents. *See generally* FBI Communication from General Counsel to All Field Offices, National Security Letter Matters (Nov. 28, 2001), *available at* http://www.aclu.org/patriot_foia/FOIA/Nov2001FBImemo.pdf; *and see Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the House Comm. on the Judiciary*, 107th Cong. 57-58 (2001) (describing the delays caused by limited NSL signature authority prior to 2001), *available at* http://www.house.gov/judiciary/75288.pdf.

112. *See* 147 CONG. REC. S11,003 (2001) (comments of Sen. Leahy). In the absence of any Senate reports on the USA PATRIOT Act, Senator Leahy, as Chairman of the Judiciary Committee, made extensive floor comments explaining the legislation. *See id. at* S10,990-S11,0015; *see also* 147 CONG. REC. S10,586 (2001) (comments of Sen. Hatch).

written certification by such government agency that such information is necessary for the agency's conduct of such investigation, activity, or analysis.[113]

Of the various revisions, those in §215 go farthest. Like the other counterintelligence authorities for transactional information, §215 incorporates the new "relevance" standard, but it lacks language limiting its application to specific types of records. Section 215 replaces the old "business records" authority in Title V of FISA with new language (italics indicate changes made by the USA PATRIOT Act):[114]

> §1861. Access to certain business records for foreign intelligence and international terrorism investigations
>
> (a) *(1)* The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order *requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or 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.*
>
> (2) *An investigation conducted under this section shall*
>
> *(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and*
>
> *(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.*

---

113. *See* 15 U.S.C. §1681v. This extraordinary provision, which has attracted surprisingly little notice, was buried in the money laundering provisions of Title III of the Act. *See* Pub. L. No. 107-56, §358(g)(1)(B), 115 Stat. 272, 327-328 (2001). Unlike other national security letters, the authority is limited to international terrorism matters, but it extends to agencies other than the FBI. The language of the provision and its position in the Act suggest that it was developed in isolation from the other changes to counterintelligence authorities. The new authority, for example, is not noted in the FBI's initial summary of the USA PATRIOT Act changes. *See supra* note 100.

114. Unless otherwise noted, citations to USA PATRIOT Act §215 hereinafter are to its provisions as codified in the U.S. Code.

(b) Each application under this section –

(1) shall be made to –

(A) a judge of the court established by section 103(a); or

(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the *production of tangible things* under this section on behalf of a judge of that court; and

(2) shall specify that the records concerned are sought for an *authorized investigation conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.*

(c) (1) Upon *an* application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application *meets* the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

(d) No *person* shall disclose to any other person (other than those *persons necessary to produce the tangible things* under this section) that the Federal Bureau of Investigation has sought or obtained *tangible things* under this section.

(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

While the old language allowed the FBI to seek "an order authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession,"[115] the new section allows an order requiring the production of "any tangible things (including books, records, papers, documents, and other items)."[116] The new language, like the new national security letter language, includes the caveat that the material sought must be "for an investigation to obtain foreign intelligence information not concerning a United States person or 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

115. Pub. L. No. 105-272, §602, 112 Stat. 2396, 2411 (1998).
116. 50 U.S.C. §1861(a)(1).

of activities protected by the first amendment to the Constitution."[117] A new paragraph curiously repeats the First Amendment constraint from the preceding paragraph.[118] The old standard that there be "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or agent of a foreign power" is replaced by a specification that the records sought be for an "authorized investigation," as defined in an earlier paragraph.[119] There are no changes to the role of the court ("the judge shall enter an ex parte order as requested"), and the changes to the non-disclosure language simply recognize the broader scope of the records sought.[120] Section 215 adds a "good faith" defense against civil liability for those who comply with the orders, and it specifies that production shall not be deemed a waiver of privileges in other proceedings or contexts.[121] The congressional notification requirements are substantially unchanged.[122]

Unfortunately, there is very little in the way of legislative history for §215. The provision appeared in the House version of the USA PATRIOT Act,[123] but its substance is discussed neither in the House report nor in any floor debate.[124] The one fact that emerges from the House materials is that §215 was a substitute for "administrative subpoena" authority that the government had originally sought.[125] The Senate record is even less illuminating, consisting only of transcripts of two floor debates.[126] However, the Senate debated an amendment to §215 offered by Senator Feingold which, though defeated, raised key criticisms that served to shape the subsequent public debate.[127]

Public criticism of the USA PATRIOT Act began almost immediately, with expressions of concern over the speed with which the legislation was produced and the lack of public hearings.[128] Some members of Congress suggested that the Administration, and particularly the Attorney General, were exploiting the chaotic post-9/11 environment to accomplish a dramatic expansion of executive branch authority.[129] Although criticism of the Act in general, and of §215 in particular, has proliferated since passage, the key issues remain those first identified in the Senate debates surrounding the

---

117. *Id.*
118. *Id.* §1861(a)(2).
119. *Id.* §1861(b)(2).
120. *Id.* §1861(c)-(d).
121. *Id.* §1861(e).
122. *Id.* §1862.
123. *See* H.R. 2975, §156, 107th Cong. (2001).
124. As legislative history, the House published a nearly 300-page transcript of the mark-up session for H.R. 2795, along with related documents. *See* H.R. REP. NO. 107-236 (Part I) (2001).
125. *See* H.R. REP. NO. 107-236 (Part 1), at 61.
126. A debate on October 11, 2001, addressed the Senate version of the Act (S. 1510). 147 CONG. REC. S10,547-S10,630. Another on October 25, 2001, considered the final version of the Act (H.R. 3162). 147 CONG. REC. S10,990-S11,059.
127. *See* 147 CONG. REC. S10,583-S10,586 (2001).
128. *See* 147 CONG. REC. S10,585 (2001) (comments of Sen. Cantwell); *supra* note 104.
129. *See, e.g.*, 147 CONG. REC. H6,762-H6,763 (2001) (comments of Rep. Waters).

Feingold amendment.[130] There are three general criticisms: (1) §215 violates the Fourth Amendment and/or various statutory protections because it allows the government to compel production of personal information without a showing of probable cause; (2) §215 is impermissibly broad, in that it allows the FBI access to information about innocent third parties upon a showing of mere relevance to an investigation; and (3) there is no effective oversight of the use of §215.

The broad scope of the "any tangible things" language prompted charges that the section violates the Fourth Amendment by "not requir[ing] the government to get a warrant or establish probable cause" before it demands "personal records or belongings" and by failing to satisfy the notice requirements of the Fourth Amendment.[131] In somewhat more muted terms, Senator Feingold emphasized the way the provision overrides state and federal laws that protect records "containing sensitive personal information such as medical records from hospitals or doctors, or educational records, or records of what books somebody has taken out of the library."[132]

Library records have emerged as the most controversial example of "tangible things" covered by §215, especially since government access to them seems to raise state law, First Amendment, and Fourth Amendment issues.[133] Library and bookseller associations are probably now the most aggressive opponents of §215, with the libraries motivated, in part, by their historical experience with FBI counterintelligence operations.[134] Not all of their legal arguments withstand a closer look, however. For example, the

---

130. *See* 147 CONG. REC. S10,583-S10,586 (2001) (debate on Sen. Feingold's proposed amendment to §215). After his amendment was rejected, Senator Feingold reiterated his concerns during the final Senate debate on the Act. *See* 147 CONG. REC. S11,019-S11,023 (2001). Senator Feingold was the only member of the Senate to vote against passage of the USA PATRIOT Act. Reports prepared by the American Civil Liberties Union subsequent to the passage of the Act incorporate and expand upon Senator Feingold's criticisms of §215. *See* Beeson & Jaffer, *supra* note 3.

131. *See* Beeson & Jaffer, *supra* note 3, at 7.

132. *See* 147 CONG. REC. S10,583-S10,584 (2001).

133. There is an extensive collection of legal pleadings, articles, and documents relating to §215 and libraries available on the American Library Association Web site, http://www.ala.org/ala/oif/ifissues/fbiyourlibrary.htm. *See also* Anne Klinefelter, *The Role of Librarians in Challenges to the USA PATRIOT Act*, 5 N.C. J.L. & TECH. 219 (2004); Kathryn Martin, Note, *The USA PATRIOT Act's Application to Library Patron Records*, 29 J. Legis. 283 (2003).

134. During the Cold War, the FBI established a counterintelligence program known as the "Library Awareness Program." FBI agents visited libraries (particularly technical and academic libraries) for the purpose of monitoring foreign intelligence officers who were exploiting open source information from library collections. FBI counterintelligence agents attempted to recruit library staff to monitor and report on "suspicious" activities by library patrons. FBI agents also sought library circulation records and other materials. When the program came to light, there was widespread opposition to it. Litigation and congressional inquiries followed and persisted into the 1980s. Despite several attempts to craft legislation to address the issues raised by this episode, Congress never enacted a federal statute protecting library records. *See generally* HERBERT N. FOERSTEL, SURVEILLANCE IN THE STACKS: THE FBI'S LIBRARY AWARENESS PROGRAM (1991).

claim that library patron records are protected by the Fourth Amendment is not convincing, even to sympathetic commentators.[135] Rather, library patron records fall squarely into the category identified in *United States v. Miller*, that is, information that ceases to be a person's "private papers" by virtue of its being handed over to a third party who may convey it to the government.[136] The Justice Department certainly espoused this view, arguing that "[a]ny 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."[137] Indeed, this same view was expressed in the congressional debate on the USA PATRIOT Act.[138]

The controversy over library records might not be nearly so acrimonious if the First and Fourth Amendment issues could be addressed by separating the names of borrowers from the titles (and by inference from the contents) of the books they borrow. Such "anonymization" of personal reading habits might be required if §215 provided access only to purely transactional information. Thus, information that would identify a library borrower, such as name and address, would be held strictly apart from a book's title. Only if intelligence analysts subsequently linked either the book or the borrower to a credible threat would the two kinds of data be re-associated, perhaps with the approval of a neutral magistrate. Given that §215 was clearly part of a set of parallel revisions to all FBI counterintelligence authorities for access to transactional information (national security letters, pen register/trap and trace, and business records), it seems reasonable to conclude that Congress saw §215 as applying only to transactional information that is not subject to constitutional protections. The limitation of §215 to transactional records also would be consistent with the historical development of FBI counterintelligence authorities sketched out in Part I.

Whatever the intention of Congress or the understanding of the executive branch, however, there is no indication in the language of §215 that it is so limited. The lack of clarity about this point has created significant confusion. The FBI, for example, notes the uncertain scope of §215 (and the problem of library records) in its legal instructions to FBI agents on the use of §215 authority.[139] In this respect, §215 parts company with the other "transactional" counterintelligence authorities, all of which specify the data to which they

---

135. *See* Klinefelter, *supra* note 133, at 225-226. *But see* Martin, *supra* note 133.

136. United States v. Miller, 425 U.S. 435, 440-442 (1976).

137. Letter from Assistant Attorney General Bryant to Senator Leahy (Dec. 23, 2002), encl. at 2, *available at* http://fas.org/irp/agency/doj/fisa/doj-fisa-patriot-122302b.pdf.

138. *See* 147 CONG. REC. S10,993 (2001) (comments of Sen. Leahy) (the Fourth Amendment "does not normally apply" to techniques such as the FISA pen register and access to records authority).

139. FBI Memorandum from General Counsel to All Field Offices, Business Records Orders Under 50 U.S.C. §1861 (Oct. 29, 2003), at 3, *available at* http://www.aclu.org/patriot_foia/2003/FBImemo_102903.pdf.

apply, either explicitly or by their incorporation into the very statutes that protect the information at issue.[140]

How did this departure from the established pattern of clear limitation to transactional information occur? I suggest that a clue is to be found in Congress's rejection of the Administration's proposal for "administrative subpoena" authority to obtain business records.[141] Congress rejected that proposal in favor of the §215 language, apparently concluding that the requirement of a court order in §215 was more protective of privacy interests.[142] In the process it may have felt that the involvement of a neutral magistrate made a limitation on the type of information less important. There are, however, some hints in the text of §215 that elements of the "administrative subpoena" proposal were simply inserted into the existing FISA business records provision. For example, the phrase "production of any tangible things (including books, records, papers, documents, and other items)"[143] closely tracks language in the Attorney General's administrative subpoena authority for use in drug investigations, which requires "production of any records (including books, papers, documents, and other tangible things)."[144] If so, Congress might have thought it was prescribing the kind of limited scope found in the administrative subpoena authorities.

Whatever the provenance of the §215 text, abandonment of the administrative subpoena option foreclosed one proven path to securing constitutionally permissible access. Administrative subpoenas have long been available to executive branch agencies, and they now exist in at least 335

---

140. *See* 12 U.S.C. §3414(a)(5)(A) (specifying "financial records"); 18 U.S.C. §2709(a) ("subscriber information and toll billing records information, or electronic communication transactional records"); 15 U.S.C. §1681u(a)-(b) ("identity of financial institutions" and "identifying information"); 50 U.S.C. §1842(a) ("pen register" and "trap and trace" information); Pub. L. No. 105-272, §602 (specifying records of "common carrier, public accommodation facility, physical storage facility, or vehicle rental facility").

141. The text of the Administration's legislative proposals is not publicly available, but it is described by various references in the legislative history and congressional debates. *See, e.g.*, H.R. REP. NO. 107-236 (Part I), at 61. In addition, a "Consultation Draft" containing a version of the Administration's proposal appears in materials prepared by the House Judiciary Committee. *See Administration's Draft Anti-Terrorism Act of 2001*, *supra* note 111, at 45-90. The Consultation Draft includes a proposed amendment to FISA that would have replaced the old business records authority with language allowing the Attorney General to require the production of any tangible things "by administrative subpoena." *Id.* at 74.

142. *See* 147 CONG. REC. S10,586 (2001) (comments of Sen. Hatch).

143. 50 U.S.C. §1861(a)(1).

144. 21 U.S.C. §876(a). Section 876 subpoenas are commonly used by the DEA and FBI, and they would serve as a logical model for a counterintelligence administrative subpoena. In the Consultation Draft prepared for the House Judiciary Committee, §876 is identified as the "model" for the Administration's business records proposal, although the draft language provided is less detailed than that found in §876. *See Administration's Draft Anti-Terrorism Act of 2001*, *supra* note 111, at 57, 74. Following enactment of the USA PATRIOT Act, a bill creating an administrative subpoena in terrorism matters (modeled explicitly on 21 U.S.C. §876) was introduced in the House but not passed. *See* Antiterrorism Tools Enhancements Act of 2003, H.R. 3037, 108th Cong., §3.

different forms.[145] There is a substantial body of case law approving the use of administrative subpoenas, including Supreme Court decisions establishing general standards.[146] A key feature of administrative subpoena authority is its bifurcation of the authority to issue (held by the agency) and the authority to enforce (held by a court).[147] This arrangement may facilitate testing the proper scope of a particular subpoena authority in court (provided the target whose records are obtained is given notice), especially if the authority is applied in a novel or controversial context.[148] Despite the diversity of administrative subpoena authorities, moreover, the distinct enforcement role of the courts, coupled with internal agency guidelines on subpoena use, dissemination of information, and compliance with other privacy or notice requirements, are effective mechanisms to police the use of administrative subpoena authority.[149]

Unlike authorities for administrative subpoenas, national security letter authorities do not include explicit enforcement mechanisms.[150] If the recipient of a national security letter refuses to comply, the government must approach a federal court for enforcement.[151] There are no reported decisions indicating that this has occurred, but if it did happen, the court could draw on existing administrative subpoena case law to resolve questions of scope and proper use.[152]

---

145. *See* U.S. Department of Justice, Office of Legal Policy, *Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities* 4-5 (May 13, 2002), *available at* http://www.usdoj.gov/olp/.

146. *See, e.g.*, United States v. LaSalle Nat'l Bank, 437 U.S. 298, 313 (1978); United States v. Powell, 379 U.S. 48, 57 (1964); Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 209 (1946).

147. *See Report to Congress on the Use of Administrative Subpoena Authorities, supra* note 145, at 7-14.

148. *See id.; see also, e.g.*, In re Sealed Case (Administrative Subpoena), 42 F.3d 1412 (D.C. Cir. 1994) (discussing the limits placed on an administrative subpoena by relevance and investigatory purpose).

149. *See Report to Congress on the Use of Administrative Subpoena Authorities, supra* note 145, at 5, 9-25 (discussing standards for enforcement, dissemination, and notice relevant to various administrative subpoena authorities).

150. *Compare* 21 U.S.C. §876(c) (providing for judicial enforcement of administrative subpoenas) *with* 12 U.S.C. §3414(a)(5), 18 U.S.C. §2709, *and* 15 U.S.C. §1681u (making no provision for judicial enforcement of national security letters).

151. *But cf.* Doe v. Ashcroft, *supra* note 69, at 47-51 (discussing the absence of a clear enforcement mechanism for national security letters). Despite the counterintelligence context, the FBI could not seek the aid of the Foreign Intelligence Surveillance Court, since that court's jurisdiction is limited to considering applications made pursuant to the FISA. *See* 50 U.S.C. §§1803(a), 1822(c).

152. There are several factors that may explain the lack of national security letter enforcement cases. Since the national security letter authorities specify the data to which they apply, and since they are directed to entities accustomed to receiving legal process (financial institutions, credit bureaus, communications providers), there may have been little occasion for controversy over the scope or application of the authority. It could also be the case that the FBI simply does not pursue enforcement in order to avoid any risk of compromising ongoing counterintelligence operations through litigation in federal courts. This situation could change as national security letter authorities are applied to a wider range of entities. *See* Intelligence

In contrast to the administrative subpoena authority sought by the Administration, the language of §215 seems to rule out an easy test of its scope. Under §215 a records custodian immediately receives a FISA Court order to provide government access to "tangible things," so failure to comply does not trigger an enforcement proceeding, but instead places the recipient in peril of being held in contempt.[153]

The second major criticism of §215 concerns the movement from the standard of "specific and articulable facts giving reason to believe" that the target is an agent of a foreign power to a standard of "relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities."[154] Critics charge that this change gives the FBI too much authority, allowing the Bureau to conduct "fishing expeditions" by seeking the records of people who are not actual targets of an investigation.[155] Some of these critics illustrate their point with hypotheticals based on imagined applications of the section.[156]

It is undeniable, of course, that the USA PATRIOT Act lowered the standards for counterintelligence collections. This change was carefully considered, however, and it apparently was influenced by the FBI's supply of examples from actual operations. Even Senator Patrick Leahy, who is generally suspicious of expanded FBI authorities,[157] found that the "FBI has made a clear case that a relevance standard is appropriate for counter-intelligence and counterterrorism investigations, as well as for criminal investigations."[158] Other members echoed the idea that counterintelligence agents pursuing terrorists should have tools at least as readily available as those open to criminal investigators.[159]

There are two additional considerations relevant to this criticism. First, the more strident critics assume that the government, in the interest of

---

Authorization Act for Fiscal Year 2004, Pub. L. No. 108-177, §374, 117 Stat. 2599, 2628 (2003) (expanding the definition of "financial institutions" to which the RFPA national security letter authority applies). While it is not an enforcement case *per se*, Doe v. Ashcroft, *supra* note 69, contains a lengthy discussion of issues surrounding the enforcement of national security letters. *Id.* at 45-83. The holding that ECPA national security letters are unconstitutional rests, in part, on the lack of any clear procedural protections or review mechanism for this authority. *Id.* at 118-119.

153. The court would have the power to punish the contempt pursuant to 18 U.S.C. §401 (2000 & Supp. II 2002). Concerning the possibility of civil disobedience, see Klinefelter, *supra* note 133, at 226.

154. *Compare* Pub. L. No. 105-272, §602 *with* 50 U.S.C. §1861(b)(2).

155. *See* Beeson & Jaffer, *supra* note 3, at 1-3; *see also* 147 CONG. REC. S10,583-S10,584, S11,022 (2001) (comments of Sen. Feingold).

156. *See, e.g.*, Beeson & Jaffer, *supra* note 3, at 1.

157. Senator Leahy prefaced his introduction of the USA PATRIOT Act with a lengthy recitation of counterintelligence abuses dating back to the 1960s and 1970s, 147 CONG. REC. S10,992-S10,994 (2001), and he referred at one point to J. Edgar Hoover's "totalitarian control" of the FBI. 147 CONG. REC. S11,015 (2001).

158. 147 CONG. REC. S10,557 (2001).

159. *See supra* note 112.

unjustified "fishing expeditions," would be willing to collect information on innocent people not truly "relevant" to any authorized investigation.[160] If this were true, however, the pre-USA PATRIOT Act standard offered no greater protection. The old version of the FISA business records authority did not require the court to find that there were "specific and articulable" facts; the government simply had to present a certification that "specific and articulable" facts existed.[161] Unlike a FISA court judge considering an application for an electronic surveillance or physical search, the judge considering a business records application was not required to examine the facts supporting the government's certification.[162] For counterintelligence access to transactional information, both before and after the USA PATRIOT Act, the determination of whether the legal standard ("specific and articulable facts" before the Act, or "relevance" after) has been met rests solely with the FBI.

Second, the permissiveness of the new "relevance" standard in allowing the collection of information about persons who are not the targets of investigations is not necessarily a dramatic departure from the pre-USA PATRIOT Act environment. The FCRA and ECPA national security letters,[163] as well as the FISA pen register/trap and trace authority,[164] allowed some collection on persons who were merely in communication with targets that met the "specific and articulable" standard. The relevance standard does, of course, broaden the scope of the collection (and the persons subject to it),[165] but its adoption is consistent with the general intention to make counter-intelligence authorities comparable to criminal investigative ones.

It may be argued that the value of pre-USA PATRIOT Act authorities as investigative tools was unduly limited by the constraints on their availability. A clear goal of counterintelligence is to identify spies and international terrorists. If an investigator has specific and articulable facts that a target is an international terrorist, she has already achieved that goal. The authorities that incorporated the "specific and articulable" standard were useful to help

---

160. *See* Beeson & Jaffer, *supra* note 3, at 1.

161. Pub. L. No. 105-272, §602.

162. *Compare* 50 U.S.C. §§1805(a), 1824(a) (judge shall enter an order authorizing electronic surveillance or physical search if the judge finds that the relevant factual standards have been met) *with* Pub. L. No. 105-272, §602 (judge shall enter an order if the FBI application contains the required certification that "specific and articulable facts" exist).

163. Pub. L. No. 104-93, §601, 109 Stat. 961, 974-975 (1996) (authorizing use of FCRA national security letter to collect information on person who "has been, or is about to be, in contact with a foreign power or an agent of a foreign power"); Pub. L. No. 103-142, §1, 107 Stat. 1491, 1491-1492 (1993) (authorizing use of ECPA national security letters to collect information on certain persons "in communication" with a foreign power or an agent of a foreign power).

164. *See* Pub. L. No. 105-272, §601, 112 Stat. 2396, 2406 (1998) (authorizing collection of pen register/trap and trace data on a communication instrument that "has been used or is about to be used in communication with" a foreign power or agent of a foreign power).

165. The new standard apparently would allow collection on persons who were relevant to the investigation but who were not necessarily in communication with the agent of a foreign power.

build "probable cause" to conduct a search or electronic surveillance of an identified target, but they did not help in the perhaps more pressing task of sorting through the target's associates to determine whether others were involved in the terrorist activity. Criminal investigators also perform this task, but they have access to compulsory legal process (grand jury or administrative subpoenas) to obtain relevant investigative information.[166] While it may appear that counterintelligence agents operated successfully under such conditions for the twenty years prior to the USA PATRIOT Act, there is a growing consensus that, whatever the FBI's capacity to deal with traditional intelligence and espionage threats, it was not properly equipped to meet the counterterrorism challenges of the late 1990s.[167]

The third major criticism of §215 is that it lacks effective oversight for the exercise of such an expansive power, in the form of judicial approval, executive branch or congressional review, or notice to surveillance targets. Critics claim that although exercise of the power requires a court order, the judge has no meaningful discretion in considering a §215 application. While the plain language of §215 directs the judge to issue the business records order if the judge finds "that the application meets the requirements" of the section,[168] the only "requirement" (aside from making the application to a FISA judge or a specially designated magistrate)[169] is that the application specify that "the records concerned are sought for an authorized investigation."[170] The language describing the judge's role is essentially the same as that found in FISA's pen register/trap and trace provisions (both the pre- and post-USA PATRIOT Act versions),[171] which appear to be derived from the criminal pen register statute.[172] The Justice Department has made statements implying that the court does exercise some discretion, but it points to no support for this proposition.[173] In the context of criminal pen registers, the United States Court of Appeals for the Tenth Circuit has found that the limited judicial review of a pen register request does not render the statute

---

166. The standard for a grand jury subpoena is not probable cause but relevance to a criminal investigation. Moreover, the relevance standard applied in the context of grand jury subpoenas is very broad. *See* United States v. R. Enterprises, Inc., 498 U.S. 292, 301 (1991) (subpoenas are not irrelevant if there is any reasonable possibility that they will produce information relevant to the general subject of the investigation).

167. *See* THE 9/11 COMMISSION REPORT, *supra* note 24, at 263-277, 350-360.

168. 50 U.S.C. §1861(c)(1).

169. *Id.* §1861(b)(1). There is no indication that the Chief Justice has ever designated a magistrate as permitted by §1861(b)(1)(B).

170. *Id.* §1861(b)(2).

171. *Id.* §1842(d)(1).

172. 18 U.S.C. §3123(a).

173. *See* Letter from Assistant Attorney General Bryant to Senator Leahy (Dec. 23, 2002), encl. at 3, *available at* http://fas.org/irp/agency/doj/fisa/doj-fisa-patriot-122302.pdf ("The FISA Court will not order the production of business records unless it can be shown that the individual for whom the records are being sought *is* related to an authorized investigation.") (emphasis in original).

unconstitutional.[174] The Court recognized, but did not decide, the question of whether, despite the language of the statute, the reviewing court could inquire into "the government's factual basis for believing" that the request is relevant.[175] The criticism of §215 on this point remains valid: the practical nature of the FISA court judge's review of a business records application remains uncertain, as does the propriety of the standard of review, in light of the broad scope of §215 authority.

The oversight criticism also manifests itself in concern over what constitutes an "investigation." Some commentators imply that the FBI can initiate investigations at will and that it can use such investigations as a pretext to "go fishing" in the great pool of personal information.[176] Such criticisms often ignore, or discount the effect of, the regulations applicable to counterintelligence activities. The FBI is only authorized to conduct counterintelligence in compliance with regulations established by the Attorney General.[177] Those regulations, in the form of guidelines, limit the subject matter of investigations,[178] set standards for the various levels of investigation,[179] and require that investigations be conducted in accordance with the Constitution and the laws of the United States.[180] The guidelines also require extensive reporting of FBI counterintelligence activities to oversight components within the Justice Department.[181] By executive order, the FBI and Justice Department also must report to the Intelligence Oversight Board, which has the authority to review intelligence activities and guidelines.[182]

---

174. United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990). The decision rested, at least in part, on the holding that pen register data are not subject to Fourth Amendment protection. *See id., citing* Smith v. Maryland, 442 U.S. 735, 739-746 (1979).

175. *Hallmark*, 911 F.2d at 402 n.3.

176. *See supra* note 155.

177. Exec. Order No. 12,333, *supra* note 12, at §1.14

178. *See* NSI Guidelines, *supra* note 17, at 6-7 (authorizing investigations to protect against defined threats to the national security).

179. *See id.* at 3. The Guidelines authorize three levels of investigative activity: threat assessments, preliminary investigations, and full investigations. The specific standards for initiating each level of investigation remain classified. *See id.* at 11-17.

180. The Guidelines provide in part:

> These Guidelines do not authorize investigating or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. Rather, all activities under these Guidelines must have a valid purpose consistent with these Guidelines, and must be carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General guidelines.

Id. at 7-8.

181. *See id.* at 14 (reporting of preliminary and full investigations), 17 (periodic summaries of full investigations), 25-27 (reporting of all information relevant to national security threats or crimes).

182. Executive Order No. 12,863 requires the reporting of intelligence activities that violate any executive orders or presidential directives to the Intelligence Oversight Board, an independent body reporting to the President's Foreign Intelligence Advisory Board. *See* Exec.

Matters relating to FBI misconduct in counterintelligence activities are subject to investigation by the FBI's Office of Professional Responsibility[183] and by the Inspector General of the Justice Department.[184] All FISA authorities and all national security letter authorities contain a congressional reporting requirement and fall within the oversight of the House and Senate intelligence committees.[185] Despite common perceptions, therefore, FBI counter-intelligence actually functions within a highly regulated environment,[186] and the language of §215 explicitly invokes such oversight.[187]

Another criticism concerns the lack in §215 of a requirement for notice to the individual whose records have been obtained. Without knowledge of the government's actions, the individual cannot challenge the legality of those actions, nor can the individual resist the further use or dissemination of records obtained.[188] Notice is not constitutionally required, however, where the government is obtaining information about a person from a third party outside the context of a criminal proceeding.[189] There is also a broad policy reason for secrecy, and this is reflected in the integration of non-disclosure provisions into all counterintelligence legal authorities.[190] Unlike criminal

---

Order No. 12,863, §2.4, 58 Fed. Reg. 48,441 (1993).

183. Attorney General Order No. 1931-94, *Jurisdiction for Investigation of Allegations of Misconduct by Department of Justice Employees*, Nov. 8, 1994, *available at* http://www.usdoj.gov/ag/readingroom/agencymisconducta.htm; *see also* Letter from Asst. Attorney General Bryant to Senator Leahy (Dec. 23, 2002), *supra* note 173, encl. at 3 (referring to investigation of a FISA matter by the Office of Professional Responsibility).

184. In particular, §1001 of the USA PATRIOT Act requires the Inspector General to report to Congress on any abuses of civil rights and civil liberties by Department of Justice employees (including the FBI). *See* Pub. L. No. 107-56, §1001, 115 Stat. 272, 391. A collection of these reports is available at http://www.usdoj.gov/oig/.

185. *See* 12 U.S.C. §3414(a)(5)(C) (RFPA national security letter); 15 U.S.C. §1681u(h) (FCRA national security letter); 18 U.S.C. §2709(c) (ECPA national security letter); 50 U.S.C. §§1808, 1826, 1846, 1862 (FISA electronic surveillance, physical search, pen register, and business records authorities).

186. This "highly regulated environment" has been in place since the late 1970s. When referring to FBI counterintelligence abuses, critics frequently cite examples from the 1960s and early 1970s. *See supra* note 157 (comments of Sen. Leahy); Beeson & Jaffer, *supra* note 3, at 9-11. Senator Leahy, referring to Exec. Order No. 12,333 and the Attorney General's Guidelines, noted the effect of the regulatory environment. 147 CONG. REC. S10,993 (2001) ("These guidelines and procedures have served for the past 25 years as a stable framework that, with rare exceptions, has not allowed previous abuses to recur.").

187. *See* 50 U.S.C. §1861(a)(2)(A) (investigations must "be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order)").

188. *See* Beeson & Jaffer, *supra* note 3, at 8.

189. *See* Securities and Exchange Comm'n v. Jerry T. O'Brien, Inc., 467 U.S. 735, 741-744 (1984).

190. *See* 12 U.S.C. §3414(a)(5)(D) (RFPA national security letter); 15 U.S.C. §1681u(d) (FCRA national security letter); 18 U.S.C. §2709(c) (ECPA national security letter), *and* 50 U.S.C. §§1805(c)(2)(B)-(C), 1824(c)(2)(B)-(C), 1842(d)(2)(B), 1861(d) (FISA electronic surveillance, physical search, pen register, and business records authorities). The non-disclosure provisions of the ECPA national security letter were recently held unconstitutional in Doe v. Ashcroft, *supra* note 69, a decision which, if upheld, would have significant implications for all the national security letter authorities cited here.

investigations, where the existence of the investigation is often known publicly, or it is widely presumed since it follows a criminal act, counterintelligence operations typically cease to exist when they are revealed.[191] The goal of counterintelligence is to detect and monitor the activities of the foreign power or its agent without the knowledge of the foreign power. If the counterintelligence operation is revealed, the government typically turns to overt tools like criminal investigations and prosecutions, immigration proceedings, administrative processes, or diplomatic activity to respond to a threat.

Secrecy has been recognized as essential since the very beginning of American intelligence operations.[192] In many respects, the regulatory scheme governing counterintelligence, the higher legal standards for counter-intelligence authorities, and even the "wall" separating intelligence and criminal law enforcement have all functioned to counter-balance and contain a tendency toward excessive secrecy in this area. The USA PATRIOT Act alters some of these constraints by lowering the legal standards for transactional information authorities and by largely dismantling the "wall." It should certainly prompt a re-examination of some secrecy provisions. However, the operational and policy concerns that consistently tipped the balance in favor of secrecy, even during the counterintelligence reforms of the 1970s, are even more pressing in the post-9/11 environment.

My goal in Section II has not been to defend §215 against its critics, but rather to place those criticisms within the larger context of the counterintelligence legal authorities and the evolution of access to transactional information. The review of history in Section I and this contextualization in Section II are intended to better inform the revision of §215 proposed below.

III. REVISING SECTION 215

Within the next year, Congress will have to decide whether or not to retain §215 (along with other parts of the USA PATRIOT Act) in its present form. The sunset clause of the Act was intended to give Congress a chance to re-

191. In enacting the non-disclosure provisions for counterintelligence authorities, Congress appeared to accept this as axiomatic. *See, e.g.*, H.R. REP. NO. 99-690(I), at 15 ("The FBI could not effectively monitor and counter the clandestine activities of hostile espionage agents and terrorists if they had to be notified that the FBI sought their financial records for a counterintelligence investigation.").

192. In often-quoted directions to some of the first American intelligence operatives, George Washington wrote: "All that remains for me to add is, that you keep the whole matter as secret as possible. For upon secrecy, success depends in most Enterprises of the kind, and for want of it, they are generally defeated, however well planned and promising a favourable issue." Letter to Elias Dayton, July 26, 1777, *reprinted in* 8 WRITINGS OF GEORGE WASHINGTON FROM THE ORIGINAL MANUSCRIPT SOURCES, 1745-1799 (John C. Kirkpatrick ed., 1931-1944), *available at http://etext.virginia.edu/toc/modeng/public/WasFi08.html*.

evaluate the necessity of these expanded authorities.[193] In the case of §215, it appears that Congress will have very little operational data upon which to base its decision.[194] The FBI and Justice Department will doubtless continue to insist that the capability provided by §215 is necessary, even if it is rarely employed. Critics of the Act will argue that the potential for abuse is so great that it should be eliminated or severely curtailed. Both sides begin from sound premises. The nature of the terrorist threat demands that our counter-intelligence legal tools be effective, flexible, and readily available. However, these tools also represent compulsory, secret government access to personal information, and therefore they should be available only under conditions that minimize their potential for abuse.

I suggest that by drawing from the evolution of these tools and other counterintelligence authorities over time, §215 can be revised to accommodate the concerns of both sides. I make two assumptions in proposing these revisions. First, I assume that the FBI will continue to have an actual need for the general capability to compel production of transactional information, beyond that already provided for in national security letter and FISA pen register authorities. Some might argue that the USA PATRIOT Act's near-complete demolition of the "wall" between counterintelligence and criminal investigations renders the "business records" authority entirely unnecessary. Now that sharing of grand jury information with the intelligence community is permitted, it could be said, counterintelligence agents who encounter the need for business records can simply use grand jury subpoenas to obtain them. I find that view unconvincing for several reasons. Although the USA PATRIOT Act permits the sharing of grand jury information under certain circumstances, it does not compel it.[195] The availability of a grand jury also depends upon the existence of an open criminal investigation; counter-intelligence operations address many situations in which there is not yet sufficient indication of criminal activity to open such an investigation.[196] Finally, although the grand jury sharing provision in the USA PATRIOT Act

---

193. *See* 147 CONG. REC. S10,991-S10,992 (2001).

194. *See supra* note 6. Although it is possible that the FBI has used §215 since September 18, 2003, the fact that the FBI made no use of the authority in the two years immediately following the September 11 attacks (presumably a period of high investigative activity) is telling.

195. *See* Pub. L. No. 107-56, §203(a) (codified at FED. R. CRIM. P. 6(e)(3)(C)). Furthermore, sharing of the most sensitive grand jury information (that identifying U.S. persons) occurs only pursuant to guidelines issued by the Attorney General. *See* Pub. L. No. 107-56, §203(c). These guidelines, finally issued by the Attorney General on September 23, 2002, allow prosecutors to place use restrictions on the information shared and to seek modifications of the guidelines for "exigent or unusual circumstances." *See* Memorandum from the Attorney General, Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons (Sept. 23, 2002), at 3, *available* at http://www.usdoj.gov/olp/section203.pdf.

196. *See* U.S. Attorney's Manual, §§9-11.010 to 9-11.120 (Sept. 1997) (describing functions and limitations of the grand jury), *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/.

is not subject to sunset, several other provisions critical to the removal of the "wall" are.[197] If they are altered or allowed to expire, the availability of criminal tools to counterintelligence agents could change radically.

My second assumption is that the §215 business records authority rarely will be used. If the authority is properly limited to transactional information, the need to invoke it should be uncommon. The most useful, and therefore frequently sought, types of transactional information are already available to the FBI through the more accessible national security letter authorities. A great deal of the remaining transactional information is subject to no legal protection at all, and it can be provided voluntarily.[198] The compulsory authority will therefore be used only when the operation of some other law, concern over civil liability, or the resistance of the records custodian prevents voluntary production. Since that authority likely will be used infrequently, creation of a more demanding process for the government could be assumed to have a relatively minor impact on operations.

My first revision to the business records authority would be to limit its application to transactional records that are truly relevant to authorized investigations. This could be accomplished by amending §1861(b)(2) and (c)(1) as follows (proposed new language in italics):

> (b) Each application under this section – . . .
> (2) shall *recite facts demonstrating* that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.
> (c) (1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds
> *(A) that the records sought are relevant to an authorized investigation conducted in accordance with subsection (a)(2), and*
> *(B) that the records sought are not subject to the protection of the Fourth Amendment of the Constitution of the United States, and are not otherwise protected from disclosure to the FBI by the laws of the United States.*

This revision would improve the statute iu several ways. First, it would restrict the application of the authority to genuiuely transactional records. Secoud, it would establish the authority of the FISA judge considering an application to assure compliance with the legal standard. Finally, the language

---

197. Section 218, which added the "significant purpose" language to FISA, is subject to the sunset provision. *See* Pub. L. No. 107-56, §§218, 224(a); *supra* note 24.

198. The FBI apparently has sought library records by voluntary production. *See* Letter from Assistant Attorney General Bryant to Senator Leahy, *supra* note 173, encl. at 2.

would accommodate other statutes controlling the privacy of particular types of information. Should Congress decide to protect library records specifically, or any body of transactional information, the business records authority could continue to function. Similarly, the language would not require alteration should the Supreme Court revisit *Miller* or otherwise modify the notion of transactional information. This new language would alleviate concerns over the scope of the authority and over the expansiveness of the "relevance" standard. The court would be in a position to detect and terminate unwarranted "fishing expeditions." Decisions of the FISA judge on these applications would be subject to review by the Foreign Intelligence Surveillance Court of Review established in §103(b) of FISA, thus allowing further refinement of the legal standard.

My second revision would address the question of notice to the person to whom the information pertains. While the counterintelligence value of the authority would vanish if notice were commonly required, there is precedent for giving the affected person notice when the government uses the information for a purpose other than counterintelligence. The other three FISA-based counterintelligence authorities (electronic surveillance, physical search, and pen register/trap and trace) all contain provisions restricting the use and dissemination of information gained through the FISA authority,[199] requiring notice to the person affected if the government intends to "enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States" information so obtained,[200] and giving the aggrieved party a specific procedure through which to challenge the use of the information in a criminal proceeding.[201] The text of these provisions could easily be inserted into the business records section, with the phrase "business records order" replacing the phrase "pen register or trap and trace device" throughout. This change would defuse some of the criticism over notice, and it would allow for the development of additional case law as application of the authority was examined in the criminal courts.[202]

---

199. 50 U.S.C. §§1806 (electronic surveillance), 1825 (physical search), 1845 (pen register/trap and trace).

200. This language, found in the pen register section, 50 U.S.C. §1845(c), is typical.

201. The procedure is designed to afford the government an opportunity to protect sensitive national security information while allowing the defendant to challenge the legality of the particular application of the FISA authority. *See, e.g.*, 50 U.S.C. §1845(e)-(h).

202. The notice and challenge provisions for FISA pen registers (50 U.S.C. §1845) have yet to be examined in the context of a criminal case, but the analogous provisions for FISA electronic surveillance (§1806) have been. *See* United States v. Isa, 923 F.2d 1300, 1305-1307 (8th Cir. 1991); United States v. Badia, 827 F.2d 1458, 1462-1464 (11th Cir. 1987); United States v. Ott, 827 F.2d 473, 475-477 (9th Cir. 1987); In re Kevork, 788 F.2d 566, 568-571 (9th Cir. 1986); United States v. Belfield, 692 F.2d 141, 143-149 (D.C. Cir. 1982); United States v. Megahey, 553 F. Supp. 1180, 1193-1194, 1196-1197 (E.D.N.Y. 1982), *aff'd sub nom.* United States v. Duggan, 743 F.2d 59 (2nd Cir. 1984); United States v. Falvey, 540 F. Supp. 1306, 1315-1316 (E.D.N.Y. 1982).

These two revisions, if adopted, would place §215 more firmly in the tradition of carefully circumscribed counterintelligence authorities. Like national security letters and the FISA pen register authority, the scope of §215 authority would then be defined as limited to transactional materials. The definition, of course, would be dynamic, shaped by the action of the courts. The authority therefore could remain flexible, while concerns about its application to protected data would be removed. The revisions would also maintain the principle that the use of counterintelligence authorities calls for greater control than does application of analogous criminal investigatory approaches. The revised authority would function at roughly the legal standard of the grand jury subpoena, but with direct, rather than indirect, judicial oversight.

The changes proposed in this article, or something like them, are essential if Congress chooses to retain §215. The law as written simply does not inspire sufficient confidence to overcome the fear of abuse. During the congressional debates on the USA PATRIOT Act, there was extensive quotation of revered patriots, led by a warning attributed to Benjamin Franklin that "if we surrender our liberty in the name of security, we shall have neither."[203] Franklin's actual words are more nuanced and present a more direct challenge to §215 in its present form: "Those who would give up essential Liberty, to purchase a little temporary safety, deserve neither Liberty nor Safety."[204] Careful attention to the actual history of counterintelligence authorities, arcane and inaccessible though it may be, will yield the raw materials needed to construct an effective, balanced authority to replace the current §215. An appropriate narrowing of the statute will both protect what is essential to our freedoms and enhance our long-term security.

---

203. *See* 147 CONG. REC. S10,991 (2001) (remarks of Sen. Leahy). *See also* 147 CONG. REC. S10,548, S11,014, S11,019 (2001) (remarks of Sen. Leahy).

204. Benjamin Franklin, Pennsylvania Assembly: Reply to the Governor, November 11, 1755, *reprinted in* 6 PAPERS OF BENJAMIN FRANKLIN 242 (Leonard W. Labaree ed., 1963), *available at* http://www.bartleby.com/73/1056.html.

Mr. NADLER. I thank the gentleman.

I now recognize Mr. Kris for 5 minutes.

TESTIMONY OF DAVID KRIS, FORMER ASSOCIATE DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. KRIS. Chairman Nadler and Ranking Member Franks, Members of the Subcommittee, thank you for inviting me to testify today.

I support new legislation in this area, and I believe that H.R. 3189 is an excellent vehicle for further discussion leading to reform. And I have submitted a few comments on the bill to your staff.

But I must say that I would go further. I believe that Congress should enact a single statute providing for national security subpoenas to replace all of the current NSL provisions.

And the principal reason for this recommendation is that it would streamline and simplify current law, which is both intricate and idiosyncratic, to the detriment of both our liberty and our security.

A single statute would also allow a well considered and global resolution of the difficult policy questions that necessarily attend the enactment of any national security subpoena or related power.

Now, I believe any new statute should satisfy 10 essential elements that are discussed in my written submission. But let me just outline three of the most important, many of which are in H.R. 3189 in one form or another.

First, I think national security subpoenas, like grand jury subpoenas, should be issued by DOJ lawyers.

Second, the subpoenas should be limited to acquiring certain specified types of foreign intelligence or other protective information.

And third and finally—and this is critically important in my view—use of the subpoenas should be governed by rigorous minimization procedures concerning acquisition, retention and dissemination of information. The absence of such procedures in current law, I think, is a very notable omission. H.R. 3189 would deal with this problem, as well, and I think it is vitally important.

So, again, I appreciate the invitation to testify, and I look forward to answering any questions.

Thank you.

[The prepared statement of Mr. Kris follows:]

PREPARED STATEMENT OF DAVID KRIS

Statement of David Kris
before the
Subcommittee on the Constitution, Civil Rights and Civil Liberties
of the House Committee on the Judiciary
Hearing on H.R. 3189, the National Security Letters Reform Act of 2007
April 15, 2008

Chairman Nadler and Ranking Member Franks, thank you for the opportunity to testify concerning national security letters (NSLs).[1] I support legislation that would replace the various NSL statutes currently used by the FBI and other federal agencies in conducting national security investigations and related activities.[2] I believe that Chairman Nadler's bill, H.R. 3189, is an excellent vehicle for further discussion leading to reform in this important area, and I have submitted comments on it to the staff.

But I would go further. I believe Congress should enact a single statute, providing for national security subpoenas, to replace all of the current NSL provisions. This would streamline and simplify current law, which is both intricate and idiosyncratic, as shown in the summary table at Tab 1. A single statute would also allow a considered, global resolution of the difficult policy questions that necessarily attend the use of any national security subpoena power.

I believe a new national security subpoena statute should contain or satisfy 10 essential elements, which are listed, and then discussed, beginning on the next page. For illustrative purposes, to present my views in more concrete terms, I have drafted a statute that reflects those 10 elements. It appears at Tab 2.[3]

Again, I appreciate your invitation to testify, and I look forward to answering any questions the Subcommittee may have. Thank you.

* * *

[1] I am testifying solely in my individual capacity, not as a representative of any former or current employer. This testimony was cleared for publication under 28 C.F.R. § 17.18.

[2] See 12 U.S.C. § 3414 (RFPA); 15 U.S.C. § 1681u (FCRAu); 15 U.S.C. § 1681v (FCRAv); 18 U.S.C. § 2709 (ECPA); 50 U.S.C. § 436 (National Security Act); cf. 50 U.S.C. § 1861 (Patriot Act Section 215).

[3] I am sure that my proposed statute could be improved or replaced by a competent drafter; I am submitting it only to illustrate the discussion in concrete terms. More generally, I stress the tentative nature of my testimony, which is in part the product of a relatively brief period of thought unaided by inside knowledge of the current operational and threat environment (I was first contacted about the possibility of testifying one week ago). My primary purpose here is to raise issues and provide technical support, not to take a strong position on any particular question.

I believe Congress should enact a single statute, providing for national security subpoenas, to replace all of the current NSL provisions. This subpoena statute should contain or satisfy the following 10 elements. It should:

(1) streamline and simplify current law, which is unnecessarily and harmfully complex;

(2) provide for subpoenas to be issued by attorneys designated by the Attorney General;

(3) make subpoenas available to all Intelligence Community agencies, as long as the subpoena is issued by a designated attorney for the government as described in (2) above, and limited to obtaining the types of information described in (5) below, and also subject, as desired, to additional limits for particular agencies (*e.g.*, CIA);

(4) allow production of any tangible thing that is subject to compelled production via grand jury subpoena;

(5) be limited to acquiring certain specified foreign intelligence information and Secret Service protective information, subject to additional limits by analogy to 50 U.S.C. § 1861(b)(2)(A) if desired;

(6) impose a nondisclosure obligation on recipients, with the usual exceptions, that expires 60 days after a written objection is received by the government, unless the government obtains an extension order from the Foreign Intelligence Surveillance Court (FISC) – an approach that should satisfy *Doe v. Gonzales*, 500 F. Supp. 2d 379 (SDNY 2007);

(7) permit motions to quash, and to enforce, subpoenas in the FISC, using the "burdensome or oppressive" standard applicable to grand jury subpoenas under Fed. R. Crim. P. 17(c) and *United States v. R. Enterprises, Inc.*, 498 U.S. 292 (1991);

(8) provide the usual sort of prospective immunity for good-faith compliance;

(9) require minimization procedures governing acquisition, retention and dissemination of information, and limits on the use of that information, along the lines of current 50 U.S.C. § 1861(g); and

(10) adhere to the traditional oversight standard in requiring (and enabling) the Attorney General to keep the Congressional Intelligence and Judiciary Committees, as well as certain other Committees, "fully informed" on a semi-annual basis, and provide for three successive annual audits by the Justice Department's Inspector General.

As noted above, a proposed statute reflecting these elements is set forth at Tab 2. Beginning on the next page, I discuss each element in more detail, and in concrete terms, by reference to the language used in the proposed statute, subject to the caveats in footnote 3 above.

* * *

1. Streamline and Simplify Current Law.

Today, there are five NSL statutes, that impose various substantive and procedural requirements, on various federal agencies, conducting various investigations or activities, seeking various kinds of information, from various types of third parties.[4] There are also other collection statutes, with their own varying standards, that overlap to some degree with the NSL statutes.[5] Some of these variations make sense, but some do not. Two recent reports from the Department of Justice's Inspector General (IG) describe the cost of such variation.[6] To cite one example, the IG reports show that FBI agents do not always appreciate the difference between a FCRAu NSL and a FCRAv NSL.[7] This means that they are sometimes slow to use these authorities, and sometimes use them incorrectly – in other words, that national security and civil liberties both suffer. The FBI itself is not primarily to blame for this; the current statutory regime is Byzantine. The intricacy results from an iterative, evolutionary legislative process, conducted over a period of many years, punctuated by September 11. Where evolution has produced such a messy result, however, Congress should impose an intelligent design.

2. Subpoenas Issued by Designated Attorneys.

The proposed statute at Tab 2 provides for national security subpoenas to replace the current regime of national security letters. These national security subpoenas would be issued by the Attorney General or a designated attorney for the government – in most cases, a Justice Department lawyer, whether at Main Justice or a U.S. Attorney's Office.[8] By requiring the involvement of DOJ attorneys, the statute mirrors practice involving grand jury subpoenas and many administrative subpoenas, and splits the difference between national security letters, which are issued by FBI agents, and Patriot Act Section 215 orders,[9] which are issued by judges. According to the recent IG reports, FBI agents have misused national security letters, and require additional oversight. In the current environment, however, Section 215's requirement for advance judicial approval seems too cumbersome for the large number of NSLs that are issued each year (nearly 50,000 issued by the FBI alone in 2006).[10]

---

[4] 12 U.S.C. § 3414 (RFPA); 15 U.S.C. § 1681u (FCRAu); 15 U.S.C. § 1681v (FCRAv); 18 U.S.C. § 2709 (ECPA); 50 U.S.C. § 436 (National Security Act).

[5] See, *e.g.*, 50 U.S.C. § 1861 (Patriot Act Section 215).

[6] See http://www.usdoj.gov/oig/special/s0803b/final.pdf (hereinafter 2008 IG NSL Report); http://www.usdoj.gov/oig/special/s0703b/final.pdf (hereinafter 2007 IG NSL Report).

[7] See 2008 IG NSL Report at 89.

[8] Under Fed. R. Crim. P. 1(b), an "attorney for the government" is defined to be: "(A) the Attorney General or an authorized assistant; (B) a United States attorney or an authorized assistant; (C) when applicable to cases arising under Guam law, the Guam Attorney General or other person whom Guam law authorizes to act in the matter; and (D) any other attorney authorized by law to conduct proceedings under these rules as a prosecutor." This would include, for example, National Security Division attorneys at Main Justice, and AUSAs in the field. Cf. *United States v. Sells Engineering, Inc.*, 463 U.S. 418, 426 & n.8 (1983).

[9] 50 U.S.C. § 1861.

[10] See 2008 IG NSL Report at 9.

There will be strong opposition to the idea that designated attorneys, rather than FBI agents or other personnel, issue the subpoenas. This opposition probably will be expressed in terms of speed and agility – *e.g.*, that Assistant U.S. Attorneys and Main Justice lawyers may be unavailable at certain times, especially in rural areas; or that even if they are available, it will take too long to contact them. This objection, however, is hard to square with (1) the extensive process already required by the FBI before an NSL may be issued, as described in the two IG reports and in comprehensive guidance issued by the FBI in 2007,[11] and (2) the fact that, in most field offices, there is only one person – the SAC – who may authorize an NSL (in the NY, DC, and LA field offices, the FBI Assistant Directors may also do so; at FBI Headquarters, a handful of other officials may do so).[12] Replacing these officials with five or more designated AUSAs in small districts, and 10 or more designated AUSAs in larger districts, as well as a reasonable number of attorneys in the National Security Division at Main Justice, would significantly expand the pool of eligible officials, and almost surely speed up the process.

3. Subpoenas Available to All Intelligence Community Agencies.

The proposed statute applies not only to the FBI, but also to any other member of the Intelligence Community that may conduct investigations or other activities (*e.g.*, analysis) under Executive Order 12333, and to the Secret Service in performing its protective functions. I recognize that the final version of any national security subpoena statute may limit the subpoena power of certain Intelligence Community agencies, such as the CIA. Those limits, however, will need to be determined by a process that requires more time and consultation than is available to me now.

Under current law, as shown in the summary table at Tab 1, two NSL statutes (FCRAu and ECPA) apply only to the FBI, while three statutes (FCRAv, the National Security Act, and RFPA) apply to the FBI and to other agencies. In particular, of those three broader statutes, FCRAv applies to any government agency authorized to conduct investigations or other intelligence activities related to international terrorism; the National Security Act applies primarily to any authorized investigative agency conducting investigations of executive branch employees with security clearances (*e.g.*, espionage investigations); and RFPA applies to any governmental authority conducting any foreign counterintelligence or affirmative intelligence activity, and to the Secret Service in performing its protective functions.

Ultimately, these restrictions depend in large part on Executive Order 12333, because – at least in the absence of statutory charters for the Intelligence Community – it prescribes the types of investigations, and investigative methods, available to each member of the Community. The proposed statute expressly refers to the executive order in an effort to simplify current law, and

---

[11] The FBI guidance is available at http://epic.org/privacy/nsl/New_NSL_Guidelines.pdf.

[12] Currently, FBI lawyers known as Chief Division Counsels (CDCs) review all NSL requests, but the recent IG reports have cast doubt on the independence of their review, in light of their reporting structure. See 2007 IG NSL Report at xliii ("We found that … some [CDCs] have been reluctant to question the predication for NSL requests or the relevance of the information sought"); 2008 IG NSL Report at 45.

to make explicit what is now implicit – i.e., that the President determines which agencies may use NSL statutes by determining which may conduct investigations or analysis related to international terrorism or other subjects specified in the current NSL statutes.

The one notable exception to the primacy of Executive Order 12333 in this area is the law enforcement proviso of the National Security Act of 1947, which provides that the CIA "shall have no police, subpoena, or law enforcement powers or internal security functions."[13] Currently, RFPA, FCRAv, and the National Security Act NSL provisions are exceptions to that general proviso for certain types of information sought in certain types of investigations. In its current baseline form, the proposed statute would eliminate these restrictions and treat the CIA like any other Intelligence Community member, subject to the limits in Executive Order 12333 – and subject to the essential requirements that the subpoena be issued by an attorney for the government designated by the Attorney General (as discussed in part 2, above), and that it seek only the kinds of information specified in the statute (as discussed in part 5, below). Even today, the CIA may engage in the "collection of foreign intelligence or counterintelligence within the United States," as long as such collection is "coordinated with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General."[14]

Recognition that CIA and DOD may issue NSLs under current law has generated controversy.[15] Granting these agencies even broader subpoena authority may be a bridge too far. If desired, CIA's (or any agency's) use of national security subpoenas could be limited or forbidden by adding appropriate language to subsection (a)(1) of the proposed statute. As a technical matter, this would not be hard to do once the substance of the limits is determined. I have not attempted it here, however, primarily because such determination may require extended consideration and consultation between the Legislative and Executive Branches. All I can do for now is flag the issue for later resolution, without taking a position.

4. Subpoenas Available for All Tangible Things Subject to Grand Jury Subpoena.

The proposed statute applies to "any tangible thing (including books, records, papers, documents, and other items)," and is meant to reach broadly, subject to the specific limits described below. For example, the word "tangible" is meant to include not only physical objects, such as a paper billing records, but also electronic records; the word is used here in much the same way as it is used in copyright law.[16]

---

[13] 50 U.S.C. § 403-4a(d)(1).

[14] Executive Order 12333 § 1.8(a). Since the executive order was issued, of course, the Director of Central Intelligence has been replaced by the Director of National Intelligence, who is not the Director of the CIA.

[15] See, *e.g.*, http://www.nytimes.com/2007/01/14/washington/14spy.html?_r=1&oref=slogin.

[16] See 17 U.S.C. § 102 (referring to work "fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device").

Although it extends to electronic data, the proposed statute would not replace FISA's current provisions authorizing surveillance using pen registers and trap and trace devices.[17] That is primarily because pen-trap surveillance collects information that is not yet in existence at the time of the court order – i.e., it imposes a continuing obligation to produce the information over a period of time – while an NSL is generally thought only to require production of information already in existence at the time it is issued. As telecommunications providers increasingly create and maintain real-time electronic billing records, of course, a series of NSLs could effectively mimic pen-trap surveillance. It therefore may make sense to reconsider the legal distinctions between them; it would be possible, for example, to modify the subpoena statute expressly to include pen-trap surveillance.

The proposed statute does not distinguish between various kinds of tangible things, as long as they are subject to production via grand jury subpoena. Thus, for example, a national security subpoena could be used to obtain information and records not subject to any of the current NSL statutes, including those from state motor vehicle agencies, hotels, landlords, storage facilities, and other entities.[18] A report by the DOJ Inspector General reveals that from 2002 to 2006, the FBI requested 16 different types of records using Patriot Act Section 215 orders, which generally are used only when NSLs are not available.[19] If desired, of course, a subset of tangible things could be carved out of the national security subpoena statute, and remain available only via court order under Patriot Act Section 215, or subject to some other substantive or procedural limit.[20]

The proposed statute begins with the phrase, "Notwithstanding any other law," primarily to eliminate uncertainty about the effect of federal or state laws that condition the disclosure of certain information via grand jury subpoena. For example, the Buckley Amendment permits disclosure of educational records "pursuant to any lawfully issued subpoena," but requires notice to the student and parents prior to such disclosure.[21] According to the recent IG report, DOJ at one point concluded that notice would likewise be required under Section 215 of the Patriot Act, because Section 215 did not purport to apply "Notwithstanding any other law."[22] The proposed

---

[17] 50 U.S.C. §§ 1841-1846.

[18] The original version of FISA's business records provision, before it was amended by Section 215 of the Patriot Act, applied to transportation common carriers, physical storage facilities, public accommodation facilities, and vehicle rental facilities. 50 U.S.C. §§ 1861-1862 (prior to Patriot Act amendment). The legislative history explains that these four categories were included in the original statute "because of their frequent use by subjects of FBI foreign intelligence and international terrorism investigations." S. Rep. No. 185, 105th Cong. 2d Sess. 29 (1998).

[19] See http://www.usdoj.gov/oig/special/s0803a/final.pdf (hereinafter 2008 IG 215 Report) at 19.

[20] See, *e.g.*, 50 U.S.C. § 1861(a)(3) (referring to "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person").

[21] 20 U.S.C. § 1232g.

[22] See http://www.usdoj.gov/oig/special/s0703a/final.pdf (hereinafter 2007 IG 215 Report) at x, xvi.

statute includes that phrase to make clear that notice would not be required, despite the Buckley Amendment or other such laws.[23]

5. Subpoenas Limited to Certain Foreign Intelligence and Protective Information.

The proposed statute applies where the tangible things sought by the subpoena constitute or contain any of the following three kinds of information:

> (1) information that relates to the ability of the United States to protect against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, sabotage or international terrorism by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power;[24]
>
> (2) information with respect to a foreign power or foreign territory that relates to the national defense or the security of the United States, or the conduct of the foreign affairs of the United States, but does not concern a United States person;[25] or
>
> (3) information relevant to the protective functions of the Secret Service as described in 18 U.S.C. §§ 3056 and 3056A, which authorize protection of the President and the Vice President (and their immediate families), visiting foreign heads of state and other distinguished foreign visitors, and certain other persons.

This standard is both somewhat narrower and somewhat broader than current law. It is narrower than current law because, with respect to information concerning U.S. persons, it requires a direct link to the protective goals set forth in the statute. Current law, by contrast, requires only that information be relevant to, or sought for, an authorized *investigation*, the precise operational scope of which is determined by the government.[26] Thus, as the FBI has advised its agents, current law is satisfied by "a reasonable belief that the information sought via the NSL either supports or weakens facts being investigated in a case."[27] Requiring a direct link between the information sought and the statutorily defined protective purposes – unmediated by the more nebulous contours of the investigation – should prevent misuse of subpoenas even if, in any given case, an investigation has improperly expanded. This may be particularly useful in curbing any real or imagined "community of interest" abuses, whereby NSLs might be used to obtain records pertaining to persons several degrees of separation removed from the subject of an investigation.

---

[23] There is a possible anomaly, involving 18 U.S.C. §§ 2703(a) and (b)(1)(B)(i), that may need to be addressed here.

[24] Cf. 50 U.S.C. § 1801(e)(1).

[25] Cf. 50 U.S.C. § 1801(c)(2). It would also be possible to expand this second category to include information concerning a U.S. person. That might require consultations between the Legislative and Executive Branches.

[26] See, *e.g.*, 15 U.S.C. § 1681u(a)-(b).

[27] See http://epic.org/privacy/nsl/New_NSL_Guidelines.pdf at 5.

If further narrowing is desired, a variation on the standard in Patriot Act Section 215 could be considered. Under that provision, tangible things are presumed to be "relevant" to an authorized investigation, and therefore subject to production via FISA Court order, if they "pertain to" any of the following: (i) a foreign power or agent of a foreign power; (ii) the activities of a "suspected" agent of a foreign power who is the subject of an authorized investigation; or (iii) an individual who is "in contact with, or known to," such a suspected agent of a foreign power.[28] Expressed in reverse – as a rebuttable presumption *against* relevance in the *absence* of one of the three scenarios – such a provision would limit possible abuses, but might still be tolerable to the government, particularly because the presumption could be rebutted as needed in particular cases.[29] On the other hand, there is some indication, in the partially redacted portions of the recent IG report on Section 215, that this provision may have led to some confusion and difficulty, in which case further discussions with the government might be required before adopting the language.[30]

In any event, the standard in the proposed subpoena statute at Tab 2 is also somewhat broader than current law because it refers not only to protection against international terrorism and clandestine intelligence activities, but also to protection against attack, sabotage, and other grave hostile acts committed by foreign powers or their agents. There is no reason to exclude the latter group of threats from the allowable purposes served by a subpoena. On the contrary, it is clearly sensible to incorporate as much as possible the existing and familiar definition of "foreign intelligence information" in 50 U.S.C. § 1801(e), which includes both groups of foreign threats to the national security.

6. Nondisclosure.

The proposed statute requires nondisclosure, subject to the usual exceptions, if a designated official makes a written finding concerning the usual enumerated harms. Persons subject to a nondisclosure obligation may at any time challenge the scope and duration of the obligation by filing a petition in the FISC. Alternatively, they may simply object to the nondisclosure obligation in writing – *e.g.*, by sending an e-mail or letter to the attorney for the government who issued the subpoena. Sixty days later, the nondisclosure obligation automatically expires unless the government has obtained a contrary order from the FISC. This approach is designed to comply with the decision in *Doe v. Gonzales*[31]; if the *Doe* decision is overturned in the Second Circuit, reversion to the procedures outlined in 18 U.S.C. § 3511 may be possible, if desired. Given the volume of national security letters – 50,000 per year – a requirement that the government seek court approval for nondisclosure in every case seems impractical; given the First Amendment requirements outlined in *Doe*, however, only a court may impose a long-term nondisclosure order. Requiring the subject of a nondisclosure obligation to object in writing before the government assumes the burden of going to court seems

[28] 50 U.S.C. § 1861(b)(2)(A)(i)-(iii).

[29] See generally Kris and Wilson, *National Security Investigations and Prosecutions* at 18-14 to 18-16 (West 2007).

[30] See 2008 IG 215 Report at 30.

[31] 500 F. Supp. 2d 379 (SDNY 2007).

tolerable under *Doe*, and will as a practical matter limit the number of cases in which a judicial order becomes necessary (because most persons subject to a nondisclosure obligation will not object). It does mean that a nondisclosure obligation may remain in effect without judicial review, but only where no person has lodged an objection. Of course, the Office of Legal Counsel and other First Amendment specialists should review this provision before it is enacted.

7. Judicial Review and Enforcement.

The proposed statute also permits motions to quash, and to enforce, subpoenas in the FISC, under the "burdensome or oppressive" standard applicable to grand jury subpoenas.[32]

8. Immunity.

The proposed statute contains a standard immunity provision for good-faith compliance.

9. Minimization and Use.

The proposed statute requires minimization procedures governing acquisition, retention and dissemination of information obtained from a subpoena, and limits the use of that information. Currently, Section 215 of the Patriot Act requires minimization procedures governing retention and dissemination of information, but not acquisition.[33] Conceptually, this is understandable, because a third party, rather than the government itself, collects information pursuant to a Section 215 order; the same is true of a subpoena. But I believe it makes sense for the Attorney General to establish procedures governing the scope of requests made by national security subpoena, so that they are narrowly tailored; such procedures are most conveniently cast as minimization procedures governing acquisition.[34]

10. Oversight.

The proposed statute follows the traditional oversight standard in requiring the government to keep the Congressional Intelligence and Judiciary Committees "fully informed" on a semi-annual basis; with respect to certain categories of information (*e.g.*, credit reports), other Committees of Congress are also to be kept fully informed (*e.g.*, the Senate Banking Committee). To assist the Attorney General in fulfilling these requirements, the statute allows him to require any other officer to provide information as may be necessary.[35] The statute also provides for three annual audits by the Justice Department's Inspector General.

* * *

---

[32] See Fed. R. Crim. P. 17(c); *United States v. R. Enterprises, Inc.*, 498 U.S. 292 (1991).

[33] 50 U.S.C. § 1861(g). I note that under USSID 18, the normal retention period for NSA raw SIGINT is five years.

[34] See Executive Order 12333 § 2.4 ("Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad").

[35] Cf. 50 U.S.C. §§ 1804(c)-(d).

Tab 1: Summary Table Comparing Current National Security Letter (NSL) Statutes

Authority	Who May Request Production?	From Whom?	Production of What?	Requirements	Dissemination	Oversight	Other
12 USC 3414 (RFPA)	Government authority authorized to conduct "foreign counter- or foreign positive-intelligence activities" [(a)(1)(A)], or "investigations of, or intelligence or counterintelligence analyses related to, international terrorism" [(a)(1)(C)]. The Secret Service [(a)(1)(B)]. The FBI. Recipient "shall comply"[1] with request from FBI[2] [(a)(5)(A)].	Requests may be made to a "financial institution" [see (a)(2)]. Financial institutions and various listed personnel "shall comply" with FBI request[2] [(a)(5)(A)]. Note: "financial institution" defined in 31 USC 5312,[3] must be at least partly located in the U.S. [(d)].	Request: "financial records"[1] [(a)(1)]. Compel: "a customer's or entity's financial records"[1] [(a)(5)(A)].	All requests under (a)(1) require certificate of RFPA compliance under 12 USC 3403(b), and must be for purposes listed in (a)(1); request by Secret Service must be for its "protective functions" [(a)(1); (a)(1)(B). (a)(2)]. FBI certifies[2] that information is sought for "foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities," with first amendment limit[4] [(a)(5)(A)].	Dissemination by FBI allowed only as provided in AG-approved NSI Guidelines, and to another federal agency only if information "clearly relevant" to its authorized responsibilities [(a)(5)(B)].	AG must "fully inform" intelligence committees [(a)(5)(C)]. Requesting authorities must "compile an annual tabulation of the occasions in which this section was used" [(a)(4)]	Emergency access to records available in certain circumstances [(b)].
15 USC 1681u (FCRAu)	The FBI. Recipient "shall" comply[1] with request from FBI[2] [(a)-(b)].	A "consumer reporting agency" [(a)-(b)].	"names and addresses of all financial institutions … at which a consumer maintains or has maintained an account" [(a)]. "identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment" [(b)]. Note: "financial institution" defined in 12 USC 3401[5] [(a)].	FBI certifies[2] compliance with FCRAu; must first determine in writing that information is sought for conduct of "authorized investigation to protect against international terrorism or clandestine intelligence activities," with first amendment limit[1] [(a)-(b)].	Dissemination outside FBI only to other federal agencies for "a foreign counterintelligence investigation," or to the relevant military department [(f)].	AG must "fully inform" intelligence and banking committees [(h)].	FBI pays the costs of production [(e)]. Also allows court order, on FBI certification,[2] for production of a "consumer report" [(c)]. Violations trigger liquidated damages and allow injunctions, and require internal disciplinary review of responsible government employee; these remedies and sanctions are exclusive [(i), (j), (l), (m)].
15 USC 1681v (FCRAv)	A "government agency authorized to conduct investigations of, or intelligence or counterintelligence	A "consumer reporting agency" [(a)].	A "consumer report of a consumer and all other information in a consumer's file" [(a)].	Certification by a designated supervisory or Senate-confirmed officer of the agency that the information sought "is necessary" for the agency's investigation of, or	N/A	AG must "fully inform" intelligence, judiciary, house financial	

Authority	Who May Request Production?	From Whom?	Production of What?	Requirements	Dissemination	Oversight	Other
	activities or analysis related to, international terrorism" [(a)]. Recipient "shall" comply with request[1] [(a)].			intelligence or counterintelligence activities or analysis related to, international terrorism [(b)].		services, and senate banking committees [(f)].	
18 USC 2709 (ECPA)	The FBI may request[2] [(b)(1)-(2)]. Recipient "shall comply with a request … made by the Director of the Federal Bureau of Investigation under subsection (b)"[1] [(a)].	A "wire or electronic communication service provider"[6] [(a)]. Note: the term "wire or electronic communication service provider" does not include a library unless it satisfies the definition in 18 USC 2515 [(f)].	Request: "name, address, length of service, and local and long distance toll billing records" and "name, address, and length of service"[1] [(b)]. Compel: "subscriber information and toll billing records information, or electronic communication transactional records"[1] [(a)].	FBI certifies that information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities," with first amendment limit[4] [(b)].	Dissemination only pursuant to AG-approved NSI guidelines and to another federal agency if "clearly relevant" to its authorized responsibilities [(d)].	Director of FBI must "fully inform" intelligence and judiciary committees [(e)].	
50 USC 436 (National Security Act)	"Any authorized investigative agency" [(a)(1)]. Recipient "shall, if the request satisfies the requirements of this section" make records available within 30 days, except for taxpayer returns and return information under 26 USC 6103[1] [(c)(1)].	Any "financial agency, financial institution, or holding company … any consumer reporting agency" [(a)(1)].	"such financial records, other financial information, and consumer reports" [(a)(1)]. "records maintained by any commercial entity within the United States pertaining to travel by an employee in the executive branch … outside the United States" [(a)(1)].	Records pertain to current or former executive branch employee who was required to consent to access for security clearance [(a)(2)(A)]; and any one of the following: (i) "reasonable grounds" that person is or may be improperly disclosing classified information to a FP or AFP; (ii) credible evidence of excessive debt or unexplained level of affluence; or (iii) person had access and opportunity to disclose information known to have been compromised [(a)(2)(B)(i)-(iii)]. Also, financial records, other financial information, and consumer reports (not travel-related records) must be "necessary to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination" [(a)(1)]. Certification by Assistant Secretary or higher of some of the requirements listed above in (a)(2)(A) and (a)(2)(B) [(a)(3)].	Dissemination outside the requesting agency only to employing agency, DOJ for LE or CI purposes, or to another federal agency if "clearly relevant" to its authorized responsibilities [(e)].	N/A	Requesting agency pays the costs of production [(d)].

Notes to Tab 1: Summary Table Comparing Current NSL Statutes

All NSLs contain fairly standard nondisclosure provisions. See 12 U.S.C. § 3414(a)(3)(A), (a)(5)(D); 15 U.S.C. § 1681u(d); 15 U.S.C. § 1681v(c); 18 U.S.C. § 2709(c); 50 U.S.C. § 436(b). The nondisclosure provisions provide for a certification from a designated official that, absent nondisclosure, "there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person." When such a certification is made, the recipient of the NSL is warned not to "disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request)" that the government has sought or obtained in the information in question. The NSL must "notify the person or entity to whom the request is directed of the nondisclosure requirement." If a recipient makes an authorized disclosure (*e.g.*, to a person whose assistance is needed to comply with the request), he must "inform such persons of any applicable nondisclosure requirement," because those persons are "subject to the same prohibitions on disclosure." At the government's request, "any person making or intending to make a disclosure" must identify the person to whom the disclosure has or will be made, except for disclosure to attorneys. Nondisclosure orders are subject to challenge under 18 U.S.C. § 3511. This nondisclosure regime has been struck down as unconstitutional under the First Amendment by decision of a district court in the Southern District of New York, *Doe v. Gonzales*, 500 F. Supp. 2d 379 (2007), which at this writing is on appeal to the Second Circuit.

All NSLs also are subject to fairly standard immunity provisions. See 12 U.S.C. 3417(c); 15 U.S.C. § 1681u(k); 15 U.S.C. § 1681v(e); 18 U.S.C. § 2703(e); 50 U.S.C. § 436(c)(2).

[1]. Most NSL statutes individually require compliance with certain requests, but under 18 U.S.C. § 3511, all requests may be enforced via court order even if compliance with the request is not specified in the NSL statute itself.

[2]. References in this table to requests or certifications from the "FBI" refer to the FBI Director, or a designated FBI official at or above the level of a Deputy Assistant Director or Special Agent in Charge.

[3]. Under 31 U.S.C. § 5312(a)(2), a "financial institution" is defined to mean: (A) an insured bank (as defined in section 3(h) of the Federal Deposit Insurance Act (12 U.S.C. 1813(h))); (B) a commercial bank or trust company; (C) a private banker; (D) an agency or branch of a foreign bank in the United States; (E) any credit union; (F) a thrift institution; (G) a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.); (H) a broker or dealer in securities or commodities; (I) an investment banker or investment company; (J) a currency exchange; (K) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments; (L) an operator of a credit card system; (M) an insurance company; (N) a dealer in precious metals, stones, or jewels; (O) a pawnbroker; (P) a loan or finance company; (Q) a travel agency; (R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money

transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system; (S) a telegraph company; (T) a business engaged in vehicle sales, including automobile, airplane, and boat sales; (U) persons involved in real estate closings and settlements; (V) the United States Postal Service; (W) an agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph; (X) a casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 which (i) is licensed as a casino, gambling casino, or gaming establishment under the laws of any State or any political subdivision of any State; or (ii) is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act); (Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or (Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

Under 31 U.S.C. 5312(c)(1), the term also includes "[a]ny futures commission merchant, commodity trading advisor, or commodity pool operator registered, or required to register, under the Commodity Exchange Act."

[4]. The First Amendment limit, which applies to certain NSL statutes, requires that the records be sought in an investigation, "provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States." In 12 U.S.C. § 3414(a)(5)(A) (RFPA), there is no antecedent reference to any "investigation" by the FBI before the First Amendment limit appears, but as a practical matter NSLs are in fact issued by the FBI only in the context of investigations.

[5]. Under 12 U.S.C. § 3401(1), a "financial institution" is defined to mean "any office of a bank, savings bank, card issuer as defined in section 1602(n) of Title 15, industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution, located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands."

[6]. A "wire or electronic communication service provider" is defined in part in 18 U.S.C. § 2510(15), which provides that "'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications." See *United States v. Biro*, 143 F.3d 1421, 1425 n.5 (11th Cir. 1998) ("The legislative history of the Electronic Communications Privacy Act of 1986 explains that '[e]xisting telephone companies and electronic mail companies are providers of electronic communications services.'").

* * *

Tab 2: Proposed National Security Subpoena Statute

Set forth below is a draft statute providing for national security subpoenas. It is designed to be modular, so that aspects can be added, subtracted, or changed without disturbing its basic structure. It is meant to begin, not end, the conversation about improving this area of the law.

50 U.S.C. § 1881: National Security Subpoenas

(a) Requirements for Subpoena. Notwithstanding any other law, the Attorney General, or an attorney for the government designated by the Attorney General, may require by subpoena the production of any tangible thing (including books, records, papers, documents, and other items), if –

(1) The subpoena is issued in an investigation or activity authorized under Executive Order 12333 or a successor order, or in a protective investigation or activity of the United States Secret Service under 18 U.S.C. §§ 3056 and 3056A;

(2) The investigation or activity is not conducted of or concerning a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States;

(3) The tangible things sought by the subpoena constitute or contain –

(A) information that relates to the ability of the United States to protect against the threats specified in section 101(e)(1);

(B) foreign intelligence information as defined by section 101(e)(2) that does not concern a United States person; or

(C) Secret Service protective information, which is defined to be information that relates to the ability of the United States to carry out the protective functions specified in 18 U.S.C. §§ 3056 and 3056A;

(4) The tangible things sought by the subpoena could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation;

(5) The subpoena describes the tangible things that are to be produced with sufficient particularity to permit them to be fairly identified;

(6) The subpoena identifies the date and place at which the tangible things must be produced, which shall allow a reasonable period of time within which the things can be assembled and made available and be no more than 500 miles from the place at which the subpoena was served; and

(7) The subpoena provides clear and conspicuous notice of the principles and procedures described in subsections (c) and (d).

(b) Service of Subpoena. A subpoena issued under this section may be served by any person designated in the subpoena to serve it. Service upon a natural person may be made by personal delivery of the subpoena to him. Service may be made upon a domestic or foreign corporation or upon a partnership or other unincorporated association which is subject to suit under a common name, by delivering the subpoena to an officer, to a managing or general agent, or to any other agent authorized by appointment or by law to receive service of process. The affidavit of the person serving the subpoena entered on a true copy thereof by the person serving it shall be proof of service.

(c) Nondisclosure Requirement: Scope. If a designated official determines in writing before service of a subpoena that nondisclosure is necessary to avoid endangering the national security of the United States, interfering with a criminal, counterterrorism, or counterintelligence investigation, interfering with diplomatic relations, or endangering the life or physical safety of any person –

(1) No person shall disclose to any other person any information concerning the subpoena other than to –

(A) those persons to whom disclosure is necessary to comply with the subpoena;

(B) an attorney to obtain legal advice or assistance with respect to the production of things in response to the subpoena; or

(C) other persons as permitted by the Attorney General or an attorney for the government designated by the Attorney General.

(2) Any person to whom disclosure is made pursuant to subsection (c)(1) shall be subject to the nondisclosure requirements described in that subsection.

(3) Any person who discloses information concerning the subpoena to a person described in subsection (c)(1) shall notify such person of the nondisclosure requirements of this subsection.

(4) At the request of the Attorney General or an attorney for the government designated by the Attorney General, any person making or intending to make a disclosure under subsection (c)(1) shall identify the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to identify an attorney to whom disclosure was made to obtain legal advice or legal assistance with respect to the subpoena.

(5) For purposes of this subsection, a designated official is the Attorney General, an attorney for the government designated by the Attorney General, the head of any executive department listed in 5 U.S.C. § 101 that contains an organization listed in or designated pursuant to 50 U.S.C. § 401a(4), or any official within such an organization

designated by the department head who has been nominated by the President and confirmed by the Senate or is at or above the level of Assistant Secretary or Special Agent in Charge.

(d) Nondisclosure Requirement: Challenge and Duration. A person subject to a nondisclosure obligation under subsection (c) may at any time file a request pursuant to subsection (f) to alter the scope or duration of the obligation. In the absence of a contrary judicial order, the obligation shall remain in effect unless at any time a person subject to it provides a written objection to the attorney who issued the subpoena (or a successor attorney), and confirms receipt of that written objection by the attorney. Sixty days after receipt of the objection is confirmed, in the absence of a contrary judicial order, the obligation shall expire as to the person who made the objection.

(e) Judicial Proceedings: In General. All judicial proceedings under this section shall be concluded as expeditiously as possible. The record of proceedings, including pleadings filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(f) Judicial Proceedings: In the FISC. The pool established by section 103(e) shall –

(1) have jurisdiction –

(A) if requested by the Attorney General or an attorney for the government designated by the Attorney General, or by any person subject to a nondisclosure obligation, to alter the scope or duration of the obligation as reasonably necessary to avoid endangering the national security of the United States, interfering with a criminal, counterterrorism, or counterintelligence investigation, interfering with diplomatic relations, or endangering the life or physical safety of any person;

(B) if requested by the Attorney General or an attorney for the government designated by the Attorney General, to issue an order requiring compliance with a subpoena, with any failure to obey the order subject to punishment as a contempt of court, and any process under this subsection allowed to be served in any judicial district in which the person or entity subject to the subpoena may be found; and

(C) if requested by the recipient of a subpoena, to quash or modify the subpoena to the extent that it is unduly burdensome or oppressive, or otherwise unlawful.

(2) within 60 days after enactment of this subsection, adopt and, consistent the protection of national security, publish procedures governing the proceedings described in subsection (f)(1). Such procedures shall –

(A) require notice and an opportunity to be heard be provided to the Attorney General or an attorney for the government designated by the Attorney General, or to the recipient of a subpoena and any other person subject to a nondisclosure obligation, as the case may be, who is not making the request;

(B) require all proceedings to be conducted in camera, and all pleadings to be filed under seal, subject to any constitutional right to an open hearing in a contempt proceeding;

(C) permit the government to file classified affidavits or other classified material ex parte; and

(D) require the judge deciding the proceeding to issue a written statement of reasons for his decision.

(g) Judicial Proceedings: Appellate Review. A party to a proceeding under subsection (f) may file a petition with the Court of Review established under section 103(b) for review of the decision issued in the proceeding not later than 7 days after the issuance of such decision. The Court of Review shall have jurisdiction to consider such petitions and shall provide for the record a written statement of the reasons for its decision. On petition for a writ of certiorari by any party to a proceeding in the Court of Review, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

(h) Immunity. Notwithstanding any Federal, State, or local law, any person, including officers, agents, and employees, receiving a subpoena under this section, who complies in good faith with the subpoena and thus produces the tangible things sought, shall not be liable in any court of any State or the United States to any customer or other person for such production or for nondisclosure of that production to the customer.

(i) Minimization Procedures.

(1) Not later than 60 days after the effective date of this section, the Attorney General shall adopt specific minimization procedures governing the acquisition, retention and dissemination of any tangible things, or information therein, sought by or received in response to a subpoena under this section. Copies of the minimization procedures shall be provided to the courts established under section 103(a) and (b), and to the Congressional committees listed in subsection (k).

(2) In this section, the term "minimization procedures" means –

(A) specific procedures that are reasonably designed in light of the purpose and technique of the particular subpoena, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate the information described in subsection (a)(3);

(B) procedures that require that nonpublicly available information, which is not information described in subsections (a)(3)(A) or (C), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand information described in subsection (a)(3)(B) or assess its importance; and

(C) notwithstanding subparagraphs (A) and (B) of this subsection, procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

(j) Use of Information. Information acquired from tangible things received in response to a subpoena under this section concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures adopted pursuant to subsection (i). No otherwise privileged information acquired from tangible things received in accordance with the provisions of this section shall lose its privileged character. No information acquired from tangible things received in response to a subpoena under this title may be used or disclosed by Federal officers or employees except for lawful purposes.

(k) Oversight. On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives, and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate, concerning all subpoenas issued under this section. In addition, with respect to any subpoena served on a consumer reporting agency as defined in the Fair Credit Reporting Act, on a semiannual basis, the Attorney General shall fully inform the Committee on Financial Services of the House of Representatives, and the Committee on Banking, Housing and Urban Affairs of the Senate. The Attorney General may require any other officer of the United States to provide information to him as may be necessary to fulfill his obligations under this subparagraph.

(*l*) Audit. For three years following the effective date of this section, the Inspector General of the Department of Justice shall perform an annual audit of the effectiveness and use, including any improper or illegal use, of the investigative authority provided under this section, and shall provide a report of that audit to the Congressional committees described in subsection (k). Not less than 30 days before the submission of a report, the Inspector General shall provide such report to the Attorney General and the Director of National Intelligence, who may provide comments to be included in the report as the Attorney General or the Director of National Intelligence may consider necessary. The reports and any comments shall be in unclassified form, but may include a classified annex.

Mr. NADLER. Thank you very much.

We will now have a round of questions, and I will recognize myself for 5 minutes to begin the questioning.

Let me ask first. We have heard that we should not go back, as the bill that I have introduced would do, to a specific and articulable fact indicating that somebody is an agent of a foreign power, because that would cut off investigations at the outset. I believe someone has testified—maybe Mr. Woods testified to that effect.

Mr. Fein, why is it safe to do that?

Mr. FEIN. Well, first of all, it does not cut off the investigation at the outset. You can have a grand jury, which has a broader mandate, because there are checks.

And specific and articulable facts are the customary way in which we conduct stop and frisk. Those situations where, short of probable cause, it is thought that an immediate danger to safety required something less than probable cause.

And there has been no showing that the stop and frisk standard, the reasonable and particularized suspicion standard, in that context has proved insufficient to protect the national security. There is no reason to think that the same standard applied, when you are trying to gather information that is important to the safety of the American people, that it should be any less effective.

Now, it is certainly to be—it is self-evident that, say, if you have no restraints on gathering information, then you can gather more information, and it is less likely anything will slip through the cracks.

Mr. NADLER. But we do not need a broad fishing expedition. Thank you.

Mr. Woods, would you comment on that?

Mr. WOODS. Yes. I think the example of a stop and frisk illustrates the difference. Stop and frisk is a physical environment. I see someone walking down the street. I am a police officer, and I decide to stop that person. I have a target, who is a known individual.

In the case of National Security Letters, and particularly in the intelligence gathering case, that is not the dominant situation. The dominant situation is, we have unknown subjects. We have generalized threat information that we need to pin down.

And when this standard was selected for National Security Letters, it very much reflected the sort of traditional, spy-catching counterintelligence that was going on at the time.

And I think, my own experience was that that did not serve as appropriate as we moved into more counterterrorism operations toward—through the end of the 1990's. And that that is what justified the change——

Mr. NADLER. Thank you.

Mr. Kris, would you comment on that?

Mr. KRIS. Well, I guess two things.

First, the grand jury standard, which has been referred to by analogy here, is actually quite broad. And a grand jury is entitled to investigate on something far less than reasonable suspicion or a specific and articulable fact. It can investigate on any kind of sus-

picion that the law is being broken, or even just to assure itself that the law is not being broken.

Second, my own view is somewhere in between these two positions. I do not necessarily support the reversion to the pre-PATRIOT Act standard.

But I think it would be useful to focus the information sought by the subpoena on the definition of foreign intelligence information in FISA, which essentially is information that is either relevant or necessary to the ability of the United States to protect against these various specified foreign threats.

Mr. NADLER. Is that so general that you could not apply it to a specific case, what you just said?

Mr. KRIS. No, I think you could—I mean, you could apply that standard to a specific case. But the value of it, I think, is that it would keep the agents focused on the ultimate goal, which is to keep us safe, unmediated by the sort of more nebulous contours of their investigation, which may expand in one direction or another.

Mr. NADLER. Thank you.

Mr. Fein, courts have ruled that the fourth amendment does not protect records held by third parties.

Do you agree with this? And what is the interest in protecting these records, if the fourth aendment does not demand a warrant?

Mr. FEIN. Well, the fourth amendment protects reasonable expectations of privacy. And whether you agree with the Smith case and some of the others, that suggest people do not have any expectation of privacy in the phone numbers they dial or in bank records, can disagree. But that is the standard they have used.

They can reverse themselves, based upon the fact that this kind of information more and more is able to be utilized to develop a footprint, if you will, a signature of someone, that was not a danger years ago before you had the Internet.

Mr. NADLER. So, would you say, in other words, that with, as Mr. Woods put it, more and more transactional information being made available, simply by the way we live our lives these days, that in fact, people, without thinking about it, do expect privacy, where perhaps the court——

Mr. FEIN. Perhaps they would, yes.

Mr. NADLER [continuing]. Didn't think about it before?

Mr. FEIN. And it is also quite clear, Mr. Chairman, that the Congress is not prohibited by the Constitution from providing greater privacy. And soon after some of these decisions on bank records, Congress did enact the Right of Financial Privacy Act that went beyond the particular fourth amendment. And I think that is the spirit of the United States Constitution.

The right to be left alone is the rule. The government has to make a strong showing for an exception.

Mr. NADLER. Thank you.

Without objection, I am going to ask one more question to Mr. Jaffer.

Can you elaborate on why it is particularly important that the gag provision be tailored? Why doesn't the first amendment—the bill tailors the gag provision. It does not eliminate it, but it tailors it in various ways.

And why doesn't the first amendment allow the government to gag an NSL recipient without any court review? Which, in effect, is what you have now, because the court review—any court review where the court has to take whatever the government says as dispositive, is not a real review, obviously, because it leaves no discretion of the court.

So, why doesn't the first amendment allow the government to gag an NSL recipient without any court review, when it is a matter of national security?

Mr. JAFFER. Well, a couple of things. Let me speak to it from my own experience representing entities or individuals that were served with National Security Letters.

In some cases, the entities that are served with National Security Letters have information about government abuse. They would like to disclose that information to the public. They would like to disclose it to Congress.

We represent one client that wanted to disclose information to Congress during the PATRIOT Act reauthorization debate, and was not permitted to do that.

So, the gag orders have a very serious effect, not just on the first amendment rights of NSL recipients, but on the public access to information about the government's use of these surveillance authorities.

But just as a matter of protecting against abuse, it is very important that there be this kind of public oversight.

And if I could just underscore a distinction that was made by one of the other panelists, between the grand jury subpoena context and the National Security Letter context, the recipients of grand jury subpoenas are ordinarily not foreclosed from disclosing to other people that they received a subpoena. And the fact that they can disclose that information serves as a kind of check against abuse. And that check is missing in the National Security Letter context.

So, it would not make sense just to take the standards that apply in the grand jury context and export them wholesale to the National Security Letter context. The contexts are quite different, because there is no check. Exactly.

Mr. FEIN. If I could just add a footnote, Mr. Chairman. You may recall in the Pentagon Papers case, the government unilaterally said you cannot—the courts have to suppress any disclosure of the Pentagon Papers, because there would be national security danger. And the Supreme Court said no. They were published, and the sky did not fall.

Mr. NADLER. Well, that is very true. Thank you.

With the indulgence of the Committee, I must note that, at a hearing of this Subcommittee, I think a week or two ago, on the state secrets issue, we had a witness here who testified that, in the—who was the brother of the plaintiff in a Supreme Court case 50 years ago, 55 years ago, that established the state secrets doctrine—that the accident report which the courts upheld as a state secret, because they revealed state secrets, she found in the incident a couple of years ago, and declassified, and there were no state secrets in it.

In fact, it was just self-serving on the part of the Administration 55 years ago to use that excuse. So, we know that that happens.

Thank you very much.

I will now recognize the gentleman from Arizona for a very flexible five minutes.

Mr. FRANKS. Well, thank you, Mr. Chairman.

Mr. Chairman, Mr. Woods wrote in his testimony that a clear goal of counterintelligence is to identify spies and international terrorists.

If an investigator has specific and articulable facts that a target is an international terrorist, then essentially, they have already achieved that goal. And I think that was extremely insightful.

One of the things we have to separate here, in my judgment, in Mr. Fein's case, he has pointed out some things that I respect very deeply, that we need to leave our citizens alone. And I believe that. But we also have a responsibility to leave them alive.

And we want to make sure that we separate those things that are directly having to do with their privacy, and these things that are just kind of—that are not fourth amendment-protected things—the information that would give us the ability to identify whether someone is a potential terrorist that then we can take to the court in the first place.

Without some of this information, we would not be able to go to a judge, because we do not have enough information even to suggest that there is any issue. The police officer cannot go to the judge before he takes a blindfold off to look at the neighborhood. We have to kind of try to get a little bit commonsense and reasonable here, in my opinion.

Mr. Woods, in your written testimony, you criticize the idea of returning to the pre-9/11 standard of specific and articulable facts. You write that the FBI counterterrorism operations will suffer if the FBI cannot expeditiously obtain relevant information in these settings, and that you think that the need for the harmonization of criminal and national security legal standards for the acquisition of transactional information remains as vital now as it was at the time of the PATRIOT Act.

Can you elaborate on that a little bit? You are very articulate, and talk to us about that.

Mr. WOODS. The reasoning behind that is reflected in your question, which is—and I tried to lay out in my testimony, and I have laid out in truly mind-numbing, fully annotated detail in my law review article attached to it—how these authorities developed. And they—the specific and articulable fact standard, as I said, worked very well in the traditional counterintelligence environment when we often worked from known individuals, intelligence officers that we had under surveillance, that we were sort of moving outward from.

It, however, began to run into difficulty in the counterterrorism environment, when you are working sort of the other direction, from INCOINT threat information, from threats that point you toward perhaps a large number of people that you need to sort through and focus very quickly on the people who are going to be relevant to the investigation.

And the problem is, when you address that sort of situation under specific and articulable facts, you did not have specific and articulable facts with reference to all of the people in that group. The information was relevant, but you were short of that standard, just as you would be short of the probable cause standard in FISA.

And so, this is the reason why the FBI came to Congress asking for the standard to be made relevant, in my view, the principal reason.

The second reason was simply the—as has been pointed out in other parts of the testimony—to make these authorities roughly equivalent to the criminal authorities, recognizing, though, that we have to do something.

And I agree with everyone that has been testifying. We have to do something about the secrecy provisions. We have to do something about retention and dissemination. But the general intent was to make these authorities roughly equivalent to criminal authorities, and make them appropriate to the threat.

And I do not think that rolling back to the old standard addresses—neither does it address the problems that were brought up in the I.G. reports, nor does it leave us well positioned to address the threat in the environment that we are encountering.

Mr. FRANKS. Mr. Chairman, I will try to squeeze one more quick question here.

Mr. Woods, in your written testimony, you also expressed deep concerns with the provision in H.R. 3189 that would prevent the use of National Security Letter information for intelligence purposes. You wrote that the sections of the bill that address the dissemination of NSL enforcement to law enforcement—information to law enforcement—would be a thoroughly unwarranted revival of the wall separating intelligence and law enforcement that operated to such a crippling effect prior to 9/11. And this is not justified by the significant—interests at stake here.

And I think that is obviously, again, an articulate point of view. And I wonder if you could elaborate on that.

Mr. WOODS. I will try to do so briefly.

The wall situation was a very complicated one. Mr. Kris and I and others could talk about it for hours.

But the difficulty I have with that provision of 3189, I think it mirrors provisions in the FISA statute, which are there for a little bit different reason. But when we did have that requirement, when we had to track FISA-derived information that might get into law enforcement channels, we very quickly got ourselves into a very complex situation that had very negative effects on counterterrorism operations prior to 9/11. And this is all documented in the 9/11 Commission Report.

I think proposing to take the same approach now in National Security Letters, which are 10 times, 20 times the number of FISAs, is essentially asking for trouble. And we are going down a road that was proven to have difficulty. And it is inconsistent with our counterterrorism strategy at the moment.

If we obtain useful information through a National Security Letter, we should be sharing it with law enforcement, with homeland security. The idea that we would hold back intelligence reports, trying to figure out if there was National Security Letter information

in it, that we would slow down the sharing of information among Homeland Security and other protective services, State and local law enforcement, is not going to help us.

And so, I think that provision needs to be looked at. And in fact, I would advocate taking it out and having—sort of defaulting to the dissemination guidelines in the attorney general's guidelines. That would make it far easier to disseminate to those entities.

Mr. FRANKS. Thank you, Mr. Chairman, and thank all of you.

Mr. NADLER. Thank you.

I now yield 5 minutes for questioning to the distinguished Chairman of the full Committee, the gentleman from Michigan.

Mr. CONYERS. Thank you, Chairman Nadler. Welcome, all witnesses.

Let us see if during my in-and-out during this hearing, Jaffer for the Nadler—and recently added Member to the bill, Conyers—proposal. Fein, for the proposal. Woods, partially for it. Kris, somewhat for it. Is that unfair characterization? Or am I giving you too much support for it than you deserve?

Mr. WOODS. I think the part of it that I do not support may well be very significant to the legislation's author. So, perhaps I am a little bit more in the——

Mr. CONYERS. I am over-complimentary this afternoon.

Mr. WOODS. But I certainly support the idea of legislation.

Mr. CONYERS. How can we get it fixed so that you could go along with Nadler, Conyers and the Chairman of the Crime Subcommittee? I mean, what would we have to do to make it, that you would say, okay? Tell me.

Mr. WOODS. I am primarily concerned with the standards. My experience with the specific and articulable fact standard showed that, to me, to be a very frustrating, clumsy standard, which was outmoded by the time I encountered it in the 1990's.

So, my principal objection is the standard. And as I said, I think the sharing with law enforcement and Homeland Security needs to be fixed, as well.

But certainly, what is—many of the other provisions of the legislation are quite good and the direction we need to go. And I am not trying to do—you know, I am certainly not here to defend the FBI over the last 3 years and what you saw in the I.G. report. I think what is in the legislation addresses that. And so, but there's a lot of it I do support.

Mr. CONYERS. Mr. Fein, how can we help him sleep more comfortably in his bed at night? How can we help Mr. Woods? How can we fix this thing up?

Mr. FEIN. Well, I think what is needed to try to test whether or not Mr. Woods' anxieties are justified is, maybe in executive session, you need people to say we could not have gotten this NSL, if there was a specific and articulable facts standard, and to show whether that is more a theoretical or a practical problem.

Because remember, this element, there is a backup here. If you want to go just for the relevant standard, which was the situation before, have a grand jury do it. Grand juries can investigate, as Mr. Kris pointed out, on virtually anything. But you have the check, one, it is more in the sunshine, and second, it is an independent branch of government that does that.

And this is the reason why you would want to keep the specific and articulable standard in, is because then you create an incentive to use more of the checks-and-balances approach than the unilateral approach. That is why the Supreme Court has explained the rule is a warrant rather than any exceptions, because you want to have an incentive to the police to use the checks and balances where at all feasible.

That is what I would suggest.

Mr. CONYERS. Thank you.

Mr. JAFFER. Mr. Conyers, could I add something to that?

Mr. CONYERS. Of course.

Mr. JAFFER. I think that the reasonable and articulable grounds standard is actually—it is a very low standard. And it just asks the FBI to provide some sort of basis for its demand for the records. It just asks the FBI to explain to somebody why it needs the records it is asking for.

And I think that if the FBI cannot articulate why it needs the records, then there is a very good question about why the FBI needs the records, or whether it should be collecting the records in the first place.

Mr. CONYERS. How do you feel about that, Mr. Fein?

Mr. FEIN. I think that is accurate. And I think there is a similar situation that arose in the U.S. Supreme Court, the case out of *Michigan, U.S. v. U.S. District Court* case. I was there at the Department of Justice at the time. It was a claim made by then-Attorney General John Mitchell, that in domestic national security situations, you did not need any judicial warrant, because it was too complex to explain national security issues to judges.

And the court unanimously said, that is nonsense. Maybe the reason you cannot articulate a national security dimension is because it is not there. And the court ruled no, if you have some genuine belief that something mischievous is afoot, you should be able to articulate it.

And I think that is exactly applicable to this standard here.

Mr. CONYERS. Now, Mr. Kris, it is your turn.

What is the reluctance, the genuine reserve that you hold back on the Nadler-Conyers-Scott approach?

Mr. KRIS. Well, I think I am somewhere in the middle here between these various witnesses.

Mr. CONYERS. Well, that is a good place to start.

Mr. KRIS. Yes, you know, just consider me the lukewarm water inbetween the fire and the ice.

First, I agree with Mr. Fein that an executive session might be helpful here, because I think these kinds of discussions in the abstract can devolve rapidly into angels on the head of a pin. These words in a vacuum are very hard to sort of get a feel for.

I, based on my now substantially outdated operational experience, have some doubts about the specific and articulable facts relating the records to a foreign power or an agent of a foreign power. I am not sure I would go quite as far in opening it up as Mr. Woods.

Again, I think here the standard that ought to apply is the same standard, essentially, that applies under FISA. The information should be essentially a subset of foreign intelligence information—

information that is relevant to our ability to protect against these threats. I think that is where the agents ought to be focused at all times.

And so, I think that is probably the right way to go. But again, I would want to have this discussion where you could really get some hard facts and some concrete examples going around.

Mr. CONYERS. Absolutely. Then you might go from lukewarm to warm. Yes. All right.

Thank you very much, Mr. Chairman.

Mr. NADLER. Thank you.

I now recognize the gentleman from Virginia for 5 minutes.

Mr. SCOTT. Thank you.

Mr. Fein, I was intrigued when you said that the judge will decide when you have a warrant. Well, the judge, really, does not really decide, because that assumes he has got both sides of the forum. It is an ex parte decision. He makes a decision based on only one side presented, but I guess that is a decision.

But let me ask you about checks and balances generally.

You know, I always thought checks and balances, as I indicated to the previous panel, checking with another branch of government. What is wrong with checking with just subordinates to see if you are doing a good job?

Mr. FEIN. Like putting the fox in charge of the chicken house.

The problem is that everyone knows that you are on a team. As part of the executive branch, I was. And you are expected to fulfill the mission of the team. And there are a thousand ways that are undetectable that someone can lose promotions, can be otherwise marginalized in their jobs, given the equivalent of a transfer to Butte, Montana, if they come up with an opinion that is not liked.

And that is just what human nature is about. That is why we do not let people be judges in their own case. Why do you have the executive branch being the judge in its own case here?

And we know the problems that can be created. You know that, because the issues concerning a device, as to the legality of waterboarding, now the department takes the position, we told the CIA interrogators this was legal. Then, if they follow it, we cannot get at them, because we are the final say on this.

And it is a very incestuous, what I would call an intellectually endogamous situation. And that is not the way you get reliable judgments. No one is infallible.

And the situation with regard to a judge ex parte deciding on warrants, it is true. He only hears one side, but he does not have a benefit like someone in law enforcement, that he gets promoted if there is an arrest made or not.

That is why, even though it is not a perfect system, it is superior to the unilateral action.

Mr. SCOTT. And why is the necessity for an outside check and balance even more important in this case, when you have the relevance to an investigation—what is the standard on these NSL—what standard are you using?

Mr. FEIN. Sir, with the current statute it is the relevance to a terrorist investigation, which is rather broad.

Mr. SCOTT. Well, you know it covers some stuff that needs to be covered. Where is the limitation?

I mean, you could almost investigate anything using that standard, it seems to me.

Is there any limitation? I mean, what is terrorist? What is relevant? Whose records?

Mr. FEIN. Well, I think you are pointing out the elusiveness of a relevance standard with regard to terrorism. You can try to connect dots all around the world. It is conceivable that something that looks innocuous 99,000 out of 99,001 times maybe turns up something, so maybe you are looking for something that is relevant. That is why it is so open-ended.

And if it is going to be that broad, the way in which we traditionally have a check is through grand jury and then the sunshine aspect after the fact, where abuses could be exposed.

Mr. SCOTT. Any definition of what a terrorist investigation is?

Mr. Woods?

Mr. WOODS. Don't forget, these National Security Letter statutes were intended and make explicit reference to the attorney general guidelines, which are now called the guidelines for national security investigations, which define in great detail—unfortunately, classified detail—the standards for opening investigations, the definitions applicable to——

Mr. SCOTT. Well, you know, that is kind of—the attorney general makes up his own guidelines, and he can investigate what he wants.

I mean, we have in the back of our minds the fact that we have not gotten a good answer to the allegations that they fired U.S. attorneys for failing to indict Democrats in time to affect an upcoming election. And these are the people who are writing their little guidelines to get at things they want.

You are getting information on people who are not charged with a crime.

Mr. WOODS. Well, the guidelines are intended to cover the collection of intelligence, which often does involve that. Intelligence officers, for example, working in this country, often go out of their way not to commit crimes, but yet, need to be surveilled, terrorist cells——

Mr. SCOTT. Now, if it is relevant to the investigation, you are getting information on the secrets of people who are not even charged with a crime, if you say that information might be relevant to somebody else's criminal activity.

Mr. WOODS. As you would in a criminal investigation, yes.

Mr. SCOTT. With a warrant.

Mr. WOODS. With a National Security Letter, as you would use a grand jury subpoena——

Mr. SCOTT. A grand jury, you have got two different branches of government working at that point.

Mr. WOODS. In theory.

Mr. SCOTT. And see, this is why we like a little oversight from somebody other than the one doing the chasing.

Mr. WOODS. I am not disagreeing on the point about oversight. I think there does need to be oversight outside the executive branch. And we have struggled with this. Congress has struggled with this for years in regulating intelligence operations. And it is difficult to do that.

But we do need it ultimately in the statute. I would favor it.

Mr. SCOTT. Well, if just I could comment, Mr. Chairman, that is why we have a FISA Court kind of in secret, at least looking over the proceedings. That is all ex parte. But at least you have got somebody in another branch of government watching what is done with these vague standards, and somebody that has the authority to put an end to it, if they are going into areas that are more shenanigans than investigation.

Mr. JAFFER. Mr. Scott, could I just add to that?

I actually think we have direct—we have direct evidence that judicial oversight in this area would be effective in a way that internal executive branch oversight is not. And I am thinking of the two cases that the ACLU brought challenging National Security Letters, one served on a library organization and the other one served on a John Doe organization.

In both of those cases, the FBI served an NSL, and then once we brought the challenge, the FBI made the decision, rather than defend the NSL before a judge, to drop the NSL. So, the FBI made the decision initially that the information was necessary. But when there was the threat of judicial review, the FBI backed down.

I think that shows that judicial oversight is effective in a way that executive branch oversight alone is not.

Mr. FEIN. Can I also add, Mr. Scott, that the need for an outside check of the National Security Letters is greater now than it would have been earlier, because Congress, given the status of the claims of executive privilege and state secrets, is not and cannot exercise oversight, because you repeatedly encounter the claim, "Can't show you this. Executive privilege." That is why the FISA oversight is a joke.

And if this body cannot, through the customary hearing process and oversight, impose a check after the fact, all the more need at the outset to have some other branch—here, the third branch of government—be involved in some way.

And I want to underscore, this is not an effort to handcuff investigations. It is saying, be muscular, but do it with checks and balances, because abuse is what happens with unilateral, unchecked power.

Mr. NADLER. The gentleman's time is well expired. We are going to have a second round of questioning, however, so he will be able to come back to these gentlemen, if he wishes.

I will now yield myself 5 minutes for further questioning.

Mr. Woods, I wanted to explore some of the distinctions you were drawing. On the one hand, you said that the particular—what was that—particularly the articulable fact standard is a two——

Mr. WOODS. Significant and articulable fact.

Mr. NADLER [continuing]. Significant and articulable—whatever it is, it is too—specific and articulable facts—it is too specific. So, I think it is too difficult.

Mr. WOODS. Yes.

Mr. NADLER. Okay. On the other hand, the relevance standard, especially when you are talking about a preliminary investigation where there is basically nothing there, seems to be completely and totally open-ended.

Could you think of some standard that might meet your practical problems, that would give us some protections that the relevance standard does not? Might we look for some other standard?

Mr. WOODS. Yes. Sure. I actually think that what Mr. Kris is talking about in terms of foreign intelligence information, and by importing that language from the FISA, is quite a reasonable requirement.

Mr. NADLER. What language is that?

Mr. WOODS. Well, what he is citing is the definition of foreign intelligence information drawn from the FISA statute. And it basically says, this is the kind of information that is relevant——

Mr. NADLER. Okay.

Mr. WOODS [continuing]. To the section of the national——

Mr. NADLER. Thank you.

Mr. Fein, you look as though——

Mr. FEIN. I cannot sustain that. Number one, if you look at the definition of national security or foreign intelligence information, it includes everything under the sun. The bank reserves in Hong Kong, you know, trade flows—that sort of thing. It is very open-ended.

And the second thing that is clearly different in FISA is that, under the standard before the Protect America Act, and I guess which has been expired, you still need probable cause to believe that your target was a foreign agent or——

Mr. NADLER. Whereas you do not need probable cause here.

Mr. FEIN [continuing]. Some lone ranger terrorist.

And there is not any such limitation with regard to the NSL.

Mr. NADLER. Mr. Jaffer, do you think there is any validity, first of all, to Mr. Woods' being upset with the significant and particular standard? And if there is, do you think we could come up with some other standard without going all the way over to relevancy, which seems to be no standard at all?

Mr. JAFFER. I think that, again, that the reasonable and articulable grounds standard is a very low standard. It is not probable cause. It just requires an articulation of a reason why the records are necessary.

And again, I think if the FBI cannot articulate that, it should not be collecting the information.

Mr. NADLER. Very good.

Mr. JAFFER. I think that the fact that it is issuing 200,000 NSLs over a 4-year period shows you how widely that power will be used, unless there is a real limit placed on it.

Mr. NADLER. Thank you.

Mr. Woods, I want to explore something else you said. You mentioned with respect to a different provision of the bill, that essentially says, if I recall correctly, that you cannot use material—information, I should say—gathered under the foreign intelligence provisions in a prosecution. You separate the law enforcement. You said that that was—what we have done pre-9/11 is a real problem.

My question is the following. The fourth amendment says you cannot wiretap or get certain information without a warrant and probable cause. Now we come along and say, but wait a minute. The fourth amendment was dealing with criminal prosecutions, but

we now have a problem with foreign spies, or with terrorists, or whatever.

In order to fight the war against terrorism, or against Soviet spies, or whoever, we will have a lower standard that does not meet the fourth amendment. But we will not use this for criminal prosecutions. We will only use it to protect ourselves. And that is how we have FISA and some of the provisions here.

If you then said, but we certainly cannot use that information, that we gathered by a lower standard than the fourth amendment standards and the probable cause standard, we cannot use that in prosecutions.

Two questions. One, has that compromised national security, because we can use it in national security investigations? And two, even if it did compromise national security, how could we use it in criminal prosecutions without violating the fourth amendment by definition?

Mr. WOODS. And your question reveals the reason for it.

Mr. NADLER. Well, let me just say, because it seems to me we have it backwards. That to say that we could not use criminal investigation-derived information for national security would endanger national security. But to say that we cannot use national security information in a criminal prosecution, I do not see how that would endanger national security.

Mr. WOODS. We have to start with FISA, as you sort of laid it out. And this prohibition of sharing FISA-derived information freely with criminal prosecution derives from the fact that the standards are different.

The standards on FISA are actually not lower than the criminal standards, they are different. They comply with the fourth amendment, the reasonableness standard of the fourth amendment. That is the whole, you know, line of court cases that come from (INAUDIBLE).

But it is not probable cause that a crime has been committed. It is probable cause that a person is an agent of a foreign power.

And so, if you want to construe that as lower, it is very vital, then, that that is not sort of fed wholesale into the criminal process. That is why the distinction is there in FISA.

The difference here is, FISA is dealing with full-blown, fourth amendment-protected content. Okay. It is stuff that is surveillance——

Mr. NADLER. NSLs, or not.

Mr. WOODS. NSLs, or not. We are talking—it seems to me that one of the problems with the discussion is, you know, the level of protection and the complexity of the protection will vary, depending on the level of intrusion involved and what is being protected.

Now, where you have content, the government entering your house and searching your papers, the government——

Mr. NADLER. Transactional is not as protected as content.

Mr. WOODS. Correct. And this is, if I could tell you the whole history of National Security Letter legislation, it is kind of the neglected stepchild of FISA. No one paid much attention to it. That is why the statute——

Mr. NADLER. We are trying to remedy that now.

Mr. WOODS. And so, there is a lot of work that needs to be done to this. But I do not think we need to build it into a replica of FISA for us to achieve——

Mr. NADLER. But you still did not answer my key question.

Mr. WOODS. Okay.

Mr. NADLER. How does saying that information gleaned from National Security Letters, issued under whatever standards they are issued, can be used for national security, but cannot be used for criminal prosecution? How does that endanger national security?

Mr. WOODS. Well, for one thing, you need to do something with that information—I mean, we need to prosecute the terrorist, or the spy, in some situations. So we need to transfer it from the national security environment into the terrorism—sorry—into the criminal environment, if there is a prosecution.

But second, if I, through the use of National Security Letters, develop, say, information about a terrorist threat, and I want to disseminate that to the people who are the first responders, the State and local law enforcement, is that dissemination to law enforcement?

Well, it is, even though it might not—you know, could that information find its way into a criminal prosecution? That is the issue that is raised.

Mr. NADLER. Thank you.

Would Mr. Fein and Mr. Jaffer comment on that?

Mr. FEIN. Number one, at least at present, oftentimes people are detained without trial. Just go to Guantanamo Bay. And the President can detain U.S. citizens as enemy combatants, and they never have a trial.

So, the idea that you have to have a trial to do something certainly is not the standard that this Administration employes.

Secondly, what is it that you can do with that national security information? You can thwart the plot. You do not have to have a criminal prosecution. It is oftentimes said by this Administration, especially, you do not want law enforcement to be backward looking. You want it to be forward looking.

So, you can foil the plot in ways that do not require——

Mr. NADLER. So, you are agreeing that, if you can use that information to foil the plot, then not giving it to law enforcement for prosecution is not a problem.

Mr. FEIN. It does not prevent the safety to the Americans that comes from preventing the terrorist act.

Now, we could call it a problem in the sense that, if you want to have and ease their way to publicize how well you are doing in criminal prosecutions, that would be useful. And moreover, there may be a difficulty, if you thwart a plot and you do not have them in prison, that they could then return to that particular fray——

So I do not want to say there is no difference. But certainly, the main idea that is promoted, that you need the intelligence to prevent the crime, not prosecute it, certainly is not disturbed.

Mr. NADLER. Thank you very much.

Once again, I have gone over my 5 minutes, and the gentleman from Arizona is recognized for a very flexible 5 minutes.

Mr. FRANKS. Well, thank you, Mr. Chairman. You are always kind in that regard. I wish we could figure out a way to bring that into philosophical terms here.

Mr. Chairman, I guess, first of all, when we are gathering information that law enforcement—it is just information that is out there—I think it is very important to make this distinction. We know that, like Pseudofed and some of these other kinds of over-the-counter drugs can be purchased and then used to make other kinds of drugs that are very, very dangerous.

If someone goes into the drugstore, they have a right to have privacy about what kind of drugs they buy. But if they buy 400 boxes of Pseudofed, that might cause law enforcement eyebrows to go up.

And if we make that to where that the law enforcement—before he can even gather that information to even look at it—to be something that would go through the standard process of probable cause, I mean, we would never get anything done. The policemen would have to go around with their eyes closed.

And I just think it is very important, as someone who believes so strongly in the foundational, constitutional principles, to make sure that we apply them in the correct way.

And Mr. Fein, in all due respect, I do not think there are any American citizens at Guantanamo. And, you know, we have got to be careful how we throw these things around.

If we apply constitutional rights to terrorists that we fight in the, say, the outland of Afghanistan, and we have got to read them their rights before we arrest them, that would pretty much do away with any ability for us to fight a war on terror. And so, we have to be somewhat practical minded here, while in keeping with the basic foundations of justice.

With that said, you know, there was a time when Congress was trying to do this in the PATRIOT Act. And when this PATRIOT Act was debated in Congress, and they changed the standard for NSLs from requiring a government statement of specific and articulable facts to one of relevance, they did so after carefully considering the FBI supplies of examples from actual operations.

And even Senator Patrick Leahy, the Democratic Chairman of the Senate Judiciary Committee, found that—this is Patrick Leahy that said, "And the FBI has made a clear case that a relevant standard is appropriate for counterintelligence and counterintelligence investigations, as well as for criminal investigations."

Now, Mr. Leahy is not my mentor, so I do not suggest that you all go out and follow his perspective in every case, but it should be something maybe for the Democrats on the Committee to consider.

So, with that, let me ask Mr. Kris, if I could. H.R. 3189 provides that, "No information acquired by a National Security Letter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advanced authorization of the attorney general."

Do you support that provision? And if you do not, why not?

Mr. KRIS. I mean, first of all, let me just say that that is not a prohibition on the use of NSL-derived information in a criminal prosecution. I sympathize with what I understand to be the rationale behind that, which is the same as the rationale behind the cor-

responding language in FISA, which is that you do not want accidental disclosure through localized criminal prosecution of information that reveals a national security investigation, which has to be kept secret for longer than might otherwise occur.

And I am in favor, I think, within the context of these, by definition, national and international investigations of some kind of centralized monitoring, because they are not just local problems the way some street crime, for example, is.

Having said that, given the volume of National Security Letters—some 50,000 a year—it might be a bit steep to ask the attorney general each time to approve the way he does, or she does, in respect to FISA applications, where there are only about 2,000 a year.

So, I mean, I sympathize with the idea behind it. I am not sure that it would be administrable. And it may be better to get at the same issue through minimization procedures, which are also part of 3189, and which I do strongly support.

Mr. FRANKS. The bill would also raise the standard for the government's access to business records in terrorism investigations by requiring that the government show "specific and articulable facts, giving reason to believe that the information or records sought by that NSL would pertain to a foreign power or an agent of a foreign power."

Mr. KRIS. Yes, as I say, I think I am sort of the lukewarm water on that. I have some concerns about that language. And I do think that the use of the definition of foreign intelligence information is right.

And I just want to point out, foreign intelligence information has two separate subsections. The one that Mr. Fein referred to with respect to Hong Kong banking information is in a second and different subsection than the one we have been talking about, which is, I think, rather rigorously defined to be information that relates to the ability of the United States to protect against sabotage, international terrorism, espionage, attack and other array of hostile acts, carried out by foreign powers or agents of foreign powers.

I mean, this is a standard that has some meat on the bones. And I think it would be a reasonable way to go. And it has the advantage—as compared, say, to the current reference to the A.G. Guidelines, which are classified—that it refers to statutory language with definitional subsections that are pretty well known and could be discussed and debated publicly, at least in the abstract.

Mr. FRANKS. Mr. Chairman, I do not know if there is time for Mr. Woods to say a word on that.

Mr. WOODS. I think the point I would make about sharing with law enforcement information—and Mr. Kris makes some excellent points on the relationship to FISA. But we have to also consider this in the context of our homeland security and counterterrorism strategy.

If I have information, threat information about something that would occur in New York City, criminal prosecution is not the first thing on my mind. The first thing I want to do is tell the NYPD.

Now, if I have to worry about, you know, is this piece of paper or e-mail that I am sending to the NYPD, does that contain Na-

tional Security Letter information? If so, do we need to go to the attorney general first?

I would just say, on the basis of practical experience, that backs up the system, and you get the situation in which that stuff is not disseminated the way I think all of us would want it to be disseminated.

And I think that is not the intent of the statute, but that is an effect. That is what I am concerned about.

Mr. NADLER. Would the gentleman yield to me for a——

Mr. FRANKS. I would. Yes, sir.

Mr. NADLER. Thank you.

Mr. Woods, following up on what you were just saying, if you have information about a plot in New York, and you want to disseminate that information to the NYPD for helping prevent it, is that for law enforcement purposes?

Mr. WOODS. Well, in one sense it is not. And you would say, well, that is not a problem. But our experience with FISA information was, if you are disseminating it to a law enforcement organization, that is dissemination to law enforcement.

It is dissemination that, once it is in that organization, it could come back in the form of—it could be used in an affidavit somewhere. It could go into the process. So, the position always was that, before you give it to the law enforcement organization, you have to clear it for law enforcement purposes.

Mr. NADLER. So, would you be happier if the provision said essentially the same thing, that you cannot disclose it for law enforcement purposes, except for antiterrorism prevention purposes, or something like that?

Mr. WOODS. I think you could craft some language to deal with the threat dissemination—the dissemination of threat information, that would probably solve this problem. I think that would be a very wise thing to consider.

Mr. NADLER. Thank you. I yield back, and I thank the gentleman.

Thank you.

I now recognize the gentleman from Virginia.

Mr. SCOTT. Thank you.

I think all the witnesses have indicated that the term "foreign intelligence" includes fights against terrorism. Mr. Fein has also suggested that it includes a lot more than that.

Let me just ask on terrorism, Mr. Kris, you indicated that terrorism—does it have to be related to a State-supported terrorist? Or can you have a free, kind of a loosely organized group of terrorists that are not State supported? Would they be included in all of this?

Mr. KRIS. Yes. Non-state-supported terrorism would be included. FISA's legislative history is pretty clear in saying you could have the Larry, Moe and Curly terrorist organization. I mean, three guys who are actually engaged in terrorism would be a terrorist group.

Mr. SCOTT. Okay. Now, you indicated two sections. When we talk about foreign intelligence for the purpose of National Security Letters, are both sections of the foreign intelligence, the terrorism part

and the trade deal part, are both of them subject to National Security Letters?

Mr. KRIS. Well, you mean currently, or what I think should be?

Mr. SCOTT. Both.

Mr. KRIS. Well, currently, it depends on—you know, there are several different NSL statutes. And it depends on which statute. But most of them are focused on international terrorism, most of the broad ones. So, they would not include the so-called affirmative foreign intelligence, the banking sort, if you want, or the foreign trade stuff.

My own view is—but then there are some statutes that do refer to the foreign trade, as long as it does not concern a U.S. person. So that basically, what some of the——

Mr. SCOTT. But what is concerning, if it is relevant to a foreign intelligence investigation, you are getting information relevant to that investigation, can you not get information, records pertaining to an innocent United States citizen?

Mr. KRIS. Well, you may, but——

Mr. SCOTT. That is what the whole NSL letter is about, isn't it?

Mr. KRIS. I may be messing this up by causing more confusion than I am resolving.

But in current law, there is a distinction between this protective information, the information you need to fight against terrorism and all these other threats, and affirmative foreign intelligence information, the sort you want to get when we are spying on them, for example, trying to get trade-related information, or what have you.

And by and large—there are a number of different laws, so I do not want to make an absolute blanket statement—by and large, the second category of affirmative foreign intelligence information in this context has to be information that does not concern a U.S. person. So, it might be, for example——

Mr. SCOTT. So, using that section, where you—the trade deal section——

Mr. KRIS. Yes.

Mr. SCOTT [continuing]. You cannot get information pertaining to an innocent United States citizen.

Mr. KRIS. Or any, guilty or innocent.

Mr. SCOTT. With an NSL.

Mr. KRIS. I mean, at least under the standard that I am talking about, I——

Mr. SCOTT. Is this should be, or is?

Mr. KRIS. Well, it is what I propose, yes. And it also has a basis in current law. But there are several different provisions of current law that have different standards, so I want to be careful——

Mr. SCOTT. Is there any provision in present law where you can get information, records of an innocent United States citizen, pertaining to an investigation—a trade deal type investigation, foreign intelligence—where you can get information on an innocent United States citizen?

Mr. KRIS. I don't think so, sir, but I mean, I——

Mr. SCOTT. Does anybody want to comment?

Mr. FEIN. I think at least under FISA—now, that is not a national security——

Mr. SCOTT. Right. Well, FISA, you have got a judge looking at it, which you have some protection.

Mr. FEIN. Yes.

Mr. JAFFER. Mr. Scott, could I just jump in on this whole discussion?

I may be misunderstanding Mr. Kris' proposal, and if I am, I apologize in advance. But if the proposal is simply to replace the current—or effectively to replace—the current relevance language in the NSL statutes with the language that is in the foreign intelligence definition, which uses the phrase "relates to," I am not sure that actually solves any of the problem that at least the ACLU is concerned about.

It does not solve the problem that the FBI can go on fishing expeditions and collect information about innocent people, many degrees removed from actual suspects. And it does not in itself solve the oversight problem, either.

Mr. SCOTT. Well, let me try to get in another question.

Is there any difference of the information you can get under FISA—anything you can get under FISA that you cannot get under—with a National Security Letter, or vice versa?

Mr. JAFFER. Yes.

Mr. SCOTT. What can you get——

Mr. JAFFER. Well, under FISA you can get all kinds of information. You can get records relating to fourth amendment activity. You can get phone calls. You can get the content of phone calls. You can get e-mails.

But National Security Letters, you can get a narrower class of information.

Now, the fact that it is a narrower class does not mean that it is a non-sensitive class or a not constitutionally protective class. But it is nonetheless a narrower class of information than is available to the FBI through FISA.

Mr. NADLER. Has the gentleman concluded?

Mr. SCOTT. Not really. But if you insist, let me ask another question. [Laughter.]

Mr. NADLER. Without objection.

Mr. SCOTT. If you find information on an innocent United States citizen in one of these investigations, what happens to that information if it turns out not to be relevant to the investigation?

Do you keep that information? Do you turn it over to—if it turns out not to be relevant, can you have a collateral criminal case?

Mr. JAFFER. I think that the OIG has documented that the information—at least the practice has been—to keep some of that information. That is one of the problems that the Inspector General identified.

Mr. SCOTT. But let me say, if you have got somebody with a terrorist trying to bomb something, and you find out somebody unrelated—that you thought might have been related was unrelated, but you tripped over some drug use, can you have a criminal investigation of that drug use?

And can you backdoor investigate drug use with these NSLs using foreign intelligence as a pretext? Can you run a criminal investigation without probable cause, just out of suspicion, not probable cause, then you know he is dirty. And so, let us do a little pre-

text and call it one of these foreign intelligence investigations, and see what we trip over?

Mr. FEIN. Well, that would seem to me to violate the act, if you could ever get inside someone's head and be able to prove that this was a pretense all along. Other than confessions, I doubt whether that is something that would ever be detected. Certainly, it is a possibility.

Mr. SCOTT. Well, we changed the standard from primary purpose to——

Mr. FEIN. Significant purpose.

Mr. SCOTT [continuing]. To a significant purpose, which suggests that if it is significant, not primary, it invites the question, well, what was the primary purpose. And in fact, the attorney general, in one answer to the question, blurted out criminal investigation without probable cause—he did not say without probable cause, but that is what he meant.

Mr. FEIN. That is exactly what the danger is of lowering the standard, is you get the criminal investigation to piggyback on an intelligence investigation, and not subject to the same constraints.

Mr. SCOTT. Without the burdensome requirement of having probable cause before you start delving into people's personal papers.

Mr. FEIN. Exactly.

Mr. WOODS. A criminal investigation can be initiated without probable cause. Criminal investigation can obtain materials that we have been talking about—transactional materials—without probable cause through the use of the grand jury subpoena.

The requirement of probable cause only attaches when I would execute a search warrant or do electronic surveillance in a criminal investigation to get to that level.

The same hierarchy applies in intelligence investigations. You know, I would use a National Security Letter, which is not a probable cause instrument, to get transactional information. I would use the FISA to conduct a search warrant or use electronic surveillance for these purposes.

It is very hard—and part of the definition that Mr. Kris has been talking about of foreign intelligence information, the purpose of that definition is to prevent FISA, the surveillance and search authority, to be used as a subterfuge for criminal investigations.

So, regardless of whether it is significant purpose or primary purpose in FISA, it still has to be for the collection of foreign intelligence.

Mr. SCOTT. Yes, but if it is a significant purpose, but the primary purpose is really trying to catch somebody that you knew was dirty, but you could not initiate a criminal investigation, because you did not have probable cause to start searching his house, but can—with an NSL and all of these other things—can do a foreign intelligence investigation and backdoor, because you do not have the probable cause problem, get subpoenas and warrants to start searching somebody's house.

Mr. WOODS. But I cannot. I cannot under FISA. I have to convince a judge to get a warrant that I am—that this person is an agent of a foreign power.

Now, if the question is, can I use the NSLs, because that does not require a judge, then I—you know, the restraint there—and this is something we have already——

Mr. NADLER. The time of the gentleman has expired. All time has expired.

I want to thank you, and I want to thank our witnesses for their testimony.

Without objection, Members will have 5 legislative days to submit any additional written questions for the witnesses, which we will forward, and ask that you answer as promptly as you can, to be made part of the record.

Without objection, the record will remain open for 5 legislative days for the submission of any other additional materials.

And again, thanking our witnesses, the hearing is adjourned.

[Whereupon, at 3:16 p.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

I

110TH CONGRESS
1ST SESSION

H. R. 3189

To establish reasonable procedural protections for the use of national security letters, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 26, 2007

Mr. NADLER (for himself, Mr. FLAKE, Mr. DELAHUNT, Mr. PAUL, Mr. MACK, Mr. BOUCHER, Mr. COHEN, Mr. ELLISON, Mr. WEXLER, Ms. HARMAN, Mr. FARR, Ms. LINDA T. SÁNCHEZ of California, Mr. SCOTT of Virginia, and Ms. WASSERMAN SCHULTZ) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on Financial Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To establish reasonable procedural protections for the use of national security letters, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Security Letters Reform Act of 2007".

SEC. 2. NATIONAL SECURITY LETTER DEFINED.

In this Act, the term "national security letter" means a request for information under one of the following provisions of law:

(1) Section 2709(a) of title 18, United States Code (to access certain communication service provider records).

(2) Section 1114(a)(5)(A) of the Right to Financial Privacy Act (12 U.S.C. 3414(a)(5)(A)) (to obtain financial institution customer records).

(3) Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) (to obtain certain financial information and consumer reports).

(4) Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) (to obtain credit agency consumer records for counterterrorism investigations).

SEC. 3. PROCEDURAL PROTECTIONS FOR NATIONAL SECURITY LETTERS.

(a) STANDARD.—A national security letter may not be issued unless the official having authority under law to issue such a letter certifies that there are specific and articulable facts giving reason to believe that the information or records sought by that letter pertain to a foreign power or agent of a foreign power.

(b) LIMITATION REGARDING FIRST AMENDMENT ACTIVITIES.—A national security letter may not be issued

in connection with an investigation of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States in accordance with the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations.

(c) OTHER LIMITATIONS.—

(1) LETTER MAY NOT CONTAIN UNREASONABLE REQUIREMENTS OR REQUIRE PRIVILEGED MATTER.—A national security letter may not—

(A) contain any requirement which would be held to be unreasonable if contained in a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation of espionage or international terrorism; or

(B) require the production of any documentary evidence which would be privileged from disclosure if demanded by a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation of espionage or international terrorism.

(2) NOTICE OF RIGHTS.—A national security letter shall provide notice of the recipient's right to seek judicial review and explain the procedures for doing so.

(d) NONDISCLOSURE.—

(1) IN GENERAL.—No recipient, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under a national security letter for 30 days after receipt of such request from the Bureau.

(2) EXCEPTION.—A recipient, or officer, employee, or agent thereof, of a national security letter may disclose that the Federal Bureau of Investigation has sought or obtained access to information or records under this section to—

(A) those persons to whom disclosure is necessary in order to comply with an order under this section; or

(B) an attorney in order to obtain legal advice regarding such order.

(3) EXTENSION.—The Director of the Federal Bureau of Investigation, or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director, may apply for an order prohibiting disclosure that the Federal Bureau of Investigation has sought or obtained access to information or records

under this section for not more than 180 days after the order is issued.

(4) JURISDICTION.—An application for an order pursuant to this subsection shall be filed in the district court of the United States in any district within which the authorized investigation that is the basis for a request pursuant to this section is being conducted.

(5) APPLICATION CONTENTS.—An application for an order pursuant to this subsection must state specific and articulable facts giving the applicant reason to believe that disclosure that the Federal Bureau of Investigation has sought or obtained access to information or records under this section will result in—

(A) endangering the life or physical safety of any person;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously endangering the national security of the United States by alerting a target, a target's associates, or the for-

eign power of which the target is an agent, of the Government's interest in the target.

(6) STANDARD.—The court may issue an ex parte order in response to an application under paragraph (3) if the court determines that the order is narrowly tailored to meet a compelling interest and that there is reason to believe that disclosure that the Federal Bureau of Investigation has sought or obtained access to information or records under this section will have one of the results described in paragraph (5).

(7) RENEWAL.—An order under this subsection may be renewed for additional periods of not more than 180 days upon another application meeting the requirements of paragraph (5) and a determination by the court that the standard of paragraph (6) continues to be met.

(8) CONFORMING AMENDMENTS.—

(A) Section 2709 of title 18, United States Code, is amended by striking subsection (c).

(B) Section 1114(a)(5) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)) is amended by striking subparagraph (D).

(C) Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended by striking subsection (d).

(D) Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) is amended by striking subsection (e).

(e) JUDICIAL REVIEW.—

(1) PETITION.—Not later than 20 days after any person receives a national security, or at any time before the return date specified in the letter, whichever period is longer, such person may file, in the district court of the United States for the judicial district within which such person resides, is found, or transacts business, a petition for such court to modify or set aside such letter. The time allowed for compliance with the letter in whole or in part as deemed proper and ordered by the court shall not run while the petition is pending in the court. The petition shall specify each ground upon which the petitioner relies in seeking relief, and may be based upon any failure of the letter to comply with this section or upon any constitutional or other legal right or privilege of such person.

(2) NONDISCLOSURE.—

(A) IN GENERAL.—A person prohibited by law from disclosing information about the national security letter may file, in the district court of the United States for the judicial district within which such person resides, is found, or transacts business, a petition for the court to set aside the nondisclosure requirement. Such petition shall specify each ground upon which the petitioner relies in seeking relief, and may be based upon any failure of the nondisclosure requirement to comply with this section or upon any constitutional or other legal right or privilege of such person.

(B) STANDARD.—The court shall set aside the nondisclosure requirement unless the court determines that the nondisclosure requirement complies with this section and does not violate any constitutional or other legal right or privilege of such person.

(3) DISCLOSURE OF CLASSIFIED MATERIAL.—In making a determination under this subsection, unless the court finds that such disclosure would not assist in determining any legal or factual issue pertinent to the case, the court shall disclose to the petitioner, the counsel of the petitioner, or both, under

the procedures and standards provided in the Classified Information Procedures Act (18 U.S.C. App.), any classified portions of the application, order, or other related materials.

(f) USE OF INFORMATION.—

(1) IN GENERAL.—

(A) CONSENT.—Information acquired from a national security letter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with this subsection.

(B) LAWFUL PURPOSE.—No information acquired by a national security letter may be used or disclosed by Federal officers or employees except for lawful purposes.

(2) DISCLOSURE FOR LAW ENFORCEMENT PURPOSES.—No information acquired by a national security letter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(3) NOTIFICATION OF INTENDED DISCLOSURE BY THE UNITED STATES.—Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States against an aggrieved person any information obtained by or derived from a national security letter, the United States shall, before the trial, hearing, or other proceeding or at a reasonable time before an effort to so disclose or so use this information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the United States intends to so disclose or so use such information.

(4) NOTIFICATION OF INTENDED DISCLOSURE BY STATE OR POLITICAL SUBDIVISION.—Whenever a State or political subdivision of a State intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the State or political subdivision against an aggrieved person any information obtained or derived from a request pursuant to this

section, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(5) MOTION TO SUPPRESS.—

(A) IN GENERAL.—Any aggrieved person against whom evidence obtained or derived from a national security letter is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, or a State or political subdivision thereof, may move to suppress the evidence obtained or derived from the request, as the case may be, on the grounds that—

(i) the information was acquired in violation of the Constitution or laws of the United States; or

(ii) the request was not in conformity with the requirements of this section.

(B) TIMING.—A motion under subparagraph (A) shall be made before the trial, hear-

ing, or other proceeding unless there was no opportunity to make such a motion or the aggrieved person concerned was not aware of the grounds of the motion.

(6) JUDICIAL REVIEW.—

(A) IN GENERAL.—Whenever—

(i) a court or other authority is notified pursuant to paragraph (3) or (4);

(ii) a motion is made pursuant to paragraph (5); or

(iii) any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to—

(I) discover or obtain materials relating to a request issued pursuant to this section; or

(II) discover, obtain, or suppress evidence or information obtained or derived from a request issued pursuant to this section;

the United States district court or, where the motion is made before another authority, the United States district court in the

same district as the authority shall, notwithstanding any other provision of law and if the Attorney General files an affidavit under oath that disclosure would harm the national security of the United States, review in camera the materials as may be necessary to determine whether the request was lawful.

(B) DISCLOSURE.—In making a determination under subparagraph (A), unless the court finds that such disclosure would not assist in determining any legal or factual issue pertinent to the case, the court shall disclose to the aggrieved person, the counsel of the aggrieved person, or both, under the procedures and standards provided in the Classified Information Procedures Act (18 U.S.C. App.), any classified portions of the application, order, or other related materials, or evidence or information obtained or derived from the order.

(7) EFFECT OF DETERMINATION OF LAWFULNESS.—

(A) UNLAWFUL ORDERS.—If the United States district court determines pursuant to paragraph (6) that the national security letter

was not in compliance with the Constitution or laws of the United States, the court may, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the request or otherwise grant the motion of the aggrieved person.

(B) LAWFUL ORDERS.—If the court determines that the request was lawful, it may deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(8) BINDING FINAL ORDERS.—Orders granting motions or requests under paragraph (6), decisions under this section that a national security letter was not lawful, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other related materials shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals or the Supreme Court.

(g) DEFINITIONS.—In this Act and in each provision of law authorizing national security letters—

(1) the term "agent of a foreign power" has the meaning given such term by section 101(b) of the

Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(b));

(2) the term "aggrieved person" means a person whose name, address, length of service, or local or long distance toll records were sought or obtained under this section; and

(3) the term "foreign power" has the meaning given such term by section 101(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(a)).

SEC. 4. CAUSE OF ACTION FOR MISUSE OF NATIONAL SECURITY LETTERS.

A person to whom records requested by a national security letter pertains may, in a civil action against any person issuing or obtaining the issuing of such letter, obtain money damages equal to the greater of the actual damages or $50,000, if the national security letter was issued contrary to law or the certification on which is was based was without factual foundation.

SEC. 5. SUNSET OF PATRIOT ACT CHANGES TO NATIONAL SECURITY LETTER AUTHORITY.

(a) IN GENERAL.—The authority to issue national security letters shall revert 5 years after the date of the enactment of this Act to that provided by law on October 25, 2001.

(b) REPORT.—Not later than the date on which the authority to issue national security letters ceases under this Act, the Attorney General shall report to Congress on whether, and if so, how, the authority to issue national security letters furthered investigations as compared to alternative methods for obtaining relevant information.

SEC. 6. MINIMIZATION PROCEDURES, DISPOSAL OF WRONGLY ACQUIRED INFORMATION, AND CONGRESSIONAL REPORTING.

(a) MINIMIZATION PROCEDURES.—The Attorney General shall establish minimization and destruction procedures to ensure that information obtained pursuant to a national security letter regarding persons that are no longer of interest in an authorized investigation is destroyed. Such procedures shall be transmitted to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate in unclassified format within 3 months of passage, and shall include—

(1) specific procedures, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning

unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that provide for the destruction of information relating to United States persons that do not reflect activity that would lead a reasonable agent or analyst to believe that the person is an agent of a foreign power as defined in 50 U.S.C. 1801(b);

(3) procedures for identifying whether the information returned in response to a national security letter exceeds the scope of the original request and further procedures for returning or destroying the superfluous information as soon as possible and before it is entered into any database or used in any way; and

(4) deadlines for destruction, minimization, or return of information described in paragraphs (1) through (3), that require such destruction, minimization, or return as soon as possible.

(b) DISPOSAL OF WRONGLY ACQUIRED INFORMATION.—Each authority of the Government shall have the duty to dispose of all private information obtained without legal authority under color of a national security letter.

(c) REPORT.—The Attorney General shall, semiannually, submit to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate a unclassified report containing—

(1) the total number of national security letters issued during the preceding six months, in unclassified form;

(2) for each of the laws authorizing national security letters, the total number of national security letters issued during the preceding six months under the authority of that law;

(3) for each of the laws authorizing national security letters, the total number of national security letters issued during the preceding six months under the authority of that law for United States persons;

(4) for each of the laws authorizing national security letters, the total number of national security letters issued during the preceding six months under the authority of each such subparagraph for non-United States persons;

(5) a description of the minimization procedures adopted by the Attorney General pursuant to subsection (e), including any changes to minimization

procedures previously adopted by the Attorney General;

(6) a summary of the challenges made by recipients of national security letters in court;

(7) a description of the extent to which information obtained with national security letters has aided investigations and an explanation of how such information has aided such investigations; and

(8) a description of the extent to which information obtained with national security letters has aided prosecutions and an explanation of how such information has been used in or aided such prosecutions.

SEC. 7. REQUIREMENTS RELATING TO CLAIMS OF EMERGENCY IN CONNECTION WITH CERTAIN NATIONAL SECURITY LETTERS.

Section 2702 of title 18, United States Code, is amended—

(1) in subsection (b), so that paragraph (8) reads as follows:

"(8) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information;";

(2) in subsection (c), so that paragraph (4) reads as follows:

"(4) to a governmental entity if the provider has a reasonable belief that an emergency involving the imminent danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;"; and

(3) so that subsection (d) reads as follows:

"(d) REPORTING OF EMERGENCY DISCLOSURES.—On a semiannual basis the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

"(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8), and a summary of the factual basis for each emergency disclosure; and

"(2) the number and type of communications the Department of Justice has received by voluntary disclosure under subsection (c) (4) , and a summary of the factual basis for each emergency disclosure.".

○

○