AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 110–385

NATIONAL SECURITY LETTERS: THE NEED FOR GREATER ACCOUNTABILITY AND OVERSIGHT

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

WEDNESDAY, APRIL 23, 2008

Serial No. J–110–86

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

42–457 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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
BENJAMIN L. CARDIN, Maryland
SHELDON WHITEHOUSE, Rhode Island

ARLEN SPECTER, Pennsylvania
ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
JOHN CORNYN, Texas
SAM BROWNBACK, Kansas
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
STEPHANIE A. MIDDLETON, *Republican Staff Director*
NICHOLAS A. ROSSI, *Republican Chief Counsel*

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Cardin, Hon. Benjamin L., a U.S. Senator from the State of Maryland	6
Feingold, Hon. Russell D., a U.S. Senator from the State of Wisconsin	5
prepared statement, letter and attachments	79
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
prepared statement	84
Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania	3
Whitehouse, Hon. Sheldon, a U.S. Senator from the State of Rhode Island	7

WITNESSES

Baker, James A., former Counsel for Intelligence Policy, Department of Justice, Washington, D.C.	8
Nojeim, Gregory T., Director, Project on Freedom, Security & Technology, Center for Democracy & Technology, Washington, D.C.	11
Woods, Michael J., former Chief, National Security Law Unit, Office of the General Counsel, Federal Bureau of Investigation, Washington, D.C.	13

QUESTIONS AND ANSWERS

Responses of Michael J. Woods to questions submitted by Senator Feingold	35

SUBMISSIONS FOR THE RECORD

American Civil Liberties Union, Caroline Fredrickson, Director, Washington Legislative Office, Washington, D.C., statement and attachments	48
Baker, James A., former Counsel for Intelligence Policy, Department of Justice, Washington, D.C., statement	66
Nojeim, Gregory T., Director, Project on Freedom, Security & Technology, Center for Democracy & Technology, Washington, D.C., statement	86
Organizations supporting the National Security Letters Reform Act, joint letter	100
Woods, Michael J., former Chief, National Security Law Unit, Office of the General Counsel, Federal Bureau of Investigation, Washington, D.C., statement	102

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

NATIONAL SECURITY LETTERS: THE NEED FOR GREATER ACCOUNTABILITY AND OVERSIGHT

WEDNESDAY, APRIL 23, 2008

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC

The Committee met, pursuant to notice, at 10:04 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Feingold, Cardin, Whitehouse, Specter, Kyl, and Sessions.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. Good morning.

When Congress last reauthorized and expanded the USA PATRIOT Act in March, 2006, I voted against it, although I voted for the first one. I stated then that I felt the administration and the Congress had missed an opportunity to get it right. But we were able to include some sunshine provisions, which has given us insight that we will use today in our examination of national security letters, or NSLs.

I have long been concerned by the scope of the authority for NSLs and the lack of accountability for their use. Thankfully, we are able to include requirements for review of the NSL program by the Inspector General when we reauthorized the PATRIOT Act. There had not been that kind of a review before.

Now, for 2 years, the reports by the Inspector General have revealed extremely troubling and widespread misuse of NSLs. The authority to issue NSLs allows the Federal Bureau of Investigation to request sensitive personal information: phone bills, e-mail transactions, bank records, credit reports, things that could basically stop a business while they try to put this all together, and do this without a judge, without a grand jury, without even having a prosecutor evaluate those requests.

In the reports, the Inspector General has found some very, very disturbing misuse of this authority. The Inspector General's report found widespread violations, including failure to comply with even the minimal authorization requirements, and more disturbingly, that the FBI requested and received information to which it was not entitled under the law. The reports found some rampant confu-

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

sion about the authorities, and virtually no checks to ensure compliance or correct mistakes.

But what I found very significant, is the Inspector General found that NSL use has grown to nearly 50,000 a year, and nearly 60 percent of those NSLs are used to find information about Americans. It is a major change in the years since 9/11. I raised these concerns publicly and privately with Director Mueller of the FBI. In fairness, the FBI has acknowledged some problems. It has issued new guidelines, new guidance, a new data system to track issuance of these NSLs.

It has also created an Office of Integrity and Compliance to ensure that there are processes and procedures in place to ensure compliance.

I believe that the Director and his staff are sincere in their efforts, but I am not persuaded that the actions taken have been enough. So we are following up on an earlier oversight hearing to ask what changes are needed to the statutory authority. Among the things that concern me are whether the law should require higher level review and approval, perhaps judicial or Department of Justice review, before NSLs can be issued.

Is a standard for issuance which requires only that it be relevant to a terrorism investigation too lenient? I mention this, because we have seen all the statistics, the sudden huge increase in the number of arrests that were related and said to be terrorism. Then when we asked the question about, if they are terrorists, why did they get a fine or 30 days in jail or 60 days in jail? Well, it turned out they were just run-of-the-mill cases that they reclassified so that the statistics were good. I want to know if that is the same thing here. Is the scope of documents available under NSLs too broad?

I'd like to hear how we can ensure that there are adequate standards for determining when private records on U.S. persons that have been collected using NSLs, how can they be retained? Actually, how can they be disseminated and used?

Simply because one of these NSLs is issued with no guidance, no checks and balances, or anything else and their name gets picked up, are they going to find some day when their kids are trying to get into college, are they blocked? If they're trying to get a job or a promotion, are they suddenly blocked and they don't know why?

Now, I commend Senator Feingold. He's been a leader on this issue. I believe his bipartisan bill, the National Security Letter Reform Act of 2007, is on the right track, particularly in its recommendation for the need for a real check on independent oversight of NSLs.

The bill would also narrow the extraordinarily broad scope of information that NSLs can acquire. They would make the standard for their issuance more rigorous. I look forward to hearing our witnesses' view on this important legislation, getting ideas from them if there are other important steps we can take.

The problem we see with NSLs is just one part of a much broader concern. We all know that the changing nature of national security threats, and particularly the threat from international terrorism, has required changes in the way the government collects

and uses intelligence, the kind of information it needs. Nobody disagrees with that.

But we have to remember what a perilous undertaking it is when the government engages in domestic spying. Americans don't like it, and for very good reason. We have a long history of abuses: the Red scare of 1919; McCarthyism; co-intel for Watergate; the recent Pentagon Talon data base program; the collected information on Quakers and other anti-war protestors.

Can you imagine the shock that must have been, those collecting that, to find that Quakers were protesting a war? Quakers always protest a war. The shock would have been if, when they did that, spying on these Quakers, if they had them saying, we're in favor of war. Now, that, that would have been worth collecting.

So if we're going to adapt our collection and use of information for Americans as a changing threat, we have to be sure to do the same for the checks and accountability mechanisms, we have to protect our liberties as Americans. The FBI's misuse of NSLs is one example of the need for clearly defined procedures and careful controls when collecting and using domestic intelligence, but we have to be just as vigilant in other areas: data mining, use of satellites to collect domestic information, biometrics, fusion centers. They are all tools for national security, but each is fraught with the potential for privacy invasions and harm to American liberties. We in the Congress have a responsibility to see how these are being used.

[The prepared statement of Senator Leahy appears as a submission for the record.]

So I am looking forward to this. Senator Specter, who I mentioned is the senior Republican on the Committee, has a long history of asking these questions of both Republicans and Democrats, and I am glad you're here.

STATEMENT OF HON. ARLEN SPECTER, A U.S. SENATOR FROM THE STATE OF PENNSYLVANIA

Senator SPECTER. Thank you, Mr. Chairman. I wouldn't be anywhere else, especially since I'm the Ranking Member and I'm really not needed here because there's such a large showing of Republican members of this Committee to handle this important issue.

This is a prized Committee, very keenly sought after by members of the U.S. Senate. If any were here, I would exhort them to attend because this is a very important matter, especially in the context of what has happened with expansion of executive authority.

Decades from now, I believe historians will look down on this period since 9/11 to the present time and beyond as an extraordinary expansion of executive power, necessary, at least to some extent, as I have stated by my votes and my positions in supporting the expansion of the PATRIOT Act.

But I am concerned when we are having hearings on national security letters and we do so in the context of the President having issued a signing statement which purports to limit the executive's responsibility to comply with Section 119, notwithstanding the fact that this was a matter negotiated. That's my recollection, confirmed by Nick Rossi, who was on my staff at the time and is now Chief Counsel.

We negotiated the oversight on review of national security letters, and then the President signs a statement in which he says that he'll interpret Section 119 in a manner consistent with the broader Article 2 powers. Well, that's not adequate. There's been expressed negotiations. This comes in the context where one of the reported incidents involves a matter where the FBI sought records under Section 215 under the order for business records from the FISA court, twice refused. Then the FBI goes to a national security letter based on the same information. Well, that sounds wrong to me. If they don't have a basis for it when it goes to a court, to come back to something they have unilateral control on, it's not exactly what Congress intends here. And all of this occurs in a context with vast, vast expansion.

When you have the President violating the Foreign Intelligence Surveillance Act, the National Security Act, requiring reports to the Intelligence Committees, on his purported authority under Article 2, never tested judicially, but violations occur on unilateral action. You have the concerns about the State Secrets Act, and the Attorney General says there will be a calamitous result, violating the President's Article 2 powers.

You have an effort to legislate under the Shield Law and letters from the FBI and the Attorney General and the Director of National Intelligence and Homeland Security that the world is going to collapse, notwithstanding the careful calculation of that statute to preserve national security interests.

The attorney/client privilege, pressed by this administration far beyond any other administration. Former Attorney General Edwin Meece and former Attorney General Richard Thornburg testified in this room that the current interpretation is inappropriate. Two principles: the government proves its case, and the constitutional right to counsel, which necessarily implies confidential privilege. But now there is an expansion of executive authority. Thank God for the courts, because it has been more than frustrating to be on this Committee and to chair it, to be Ranking Member, and not to have the semblance of effective oversight. We simply can't chase the executive sufficiently to have effective oversight.

Now there is a move to have retroactive immunity to the telephone companies. As yet on the record we don't know what that retroactive immunity is for, but we're asked to grant it legislatively. I believe that from what I know as to what the telephone companies have done, they've been good citizens and they ought to be protected. But the government can step into their shoes and defend those cases and preserve the open courts, and also to give the telephone companies their due.

So I would say, Mr. Chairman, we ought to do a lot more, but I'm not quite sure what to do.

Chairman LEAHY. Well, if the Senator would yield, I was somewhat concerned when I became Chairman. I'd send letters down to Department of Justice asking questions and not get any response, and wondered if it was because I was a Democrat and it was a Republican administration. Then I found out that the chairman, when he was chairman, found it difficult to get answers to those letters also.

Senator SPECTER. Well, I'm still co-signing the letters, Mr. Chairman.

Chairman LEAHY. I know you are, and I appreciate that very much. I think oversight—I agree with the Senator from Pennsylvania. Oversight is extremely important because if you have no check and balance, at a time when our government can be all-powerful, it is a terrible situation. The Senator from Pennsylvania, like myself, was a prosecutor. There are a lot of things we would have loved to have done unilaterally. But fortunately we couldn't. We had to have oversight by the courts, we had to have checks and balances. The country's safer that way.

Senator SPECTER. I want to associate myself with the remarks which you made, following the interruption, and conclude my statement just by associating myself.

Chairman LEAHY. I apologize. I thought you had. I thought you had.

Senator SPECTER. Oh, no you don't. It's fine. We do it all the time and it's totally acceptable.

Chairman LEAHY. You see? What you all missed was the opportunity to see Senator Specter and myself at a hearing in Vermont.

Senator SPECTER. Where was everybody?

Chairman LEAHY. It was very interesting. They're still talking about it up there, approvingly.

Senator SPECTER. It was an official Committee hearing. Where was everybody?

Chairman LEAHY. And Senator Specter was praised by Republicans and Democrats across the political spectrum for his participation.

Senator Feingold, this is your legislation. If you want to say something, please feel free.

STATEMENT OF HON. RUSSELL D. FEINGOLD, A U.S. SENATOR FROM THE STATE OF WISCONSIN

Senator FEINGOLD. Thank you, Mr. Chairman and Ranking Member Specter. Thank you for holding this important hearing, and for your commitment to this issue.

I could not agree more that greater oversight and accountability are needed with respect to national security letters. The Justice Department's Inspector General documented serious misuse and abuse of national security letters from 2003 to 2006.

A followup audit conducted by the FBI itself not only confirmed the Inspector General's findings, it documented even more violations. These widespread problems are directly attributable to the PATRIOT Act, which expanded the NSL statutes to essentially grant the FBI a blank check to obtain sensitive information about innocent Americans.

Congress gave the FBI very few rules to follow and then failed to adequately fix these problems when it reauthorized the PATRIOT Act. I appreciate that Director Mueller and others in the FBI leadership ranks have taken these problems seriously, but leaving this to the FBI alone to fix is not the answer. These Inspector General reports prove that "trust us" simply doesn't cut it.

It was a significant mistake for Congress to grant the government broad powers and just keep its fingers crossed that they

wouldn't be misused. Congress has the responsibility to put appropriate limits on government powers, limits that allow agents to actively pursue criminals, terrorists, and spies, but that also protect the privacy of innocent Americans.

Congress must also ensure that the statute complies with the Constitution. In that vein, last fall a Federal District Court struck down one of the new NSL statutes, as modified by the PATRIOT Act Reauthorization legislation enacted in 2006 on First Amendment grounds.

This is why I introduced the National Security Letter Reform Act with a bipartisan group of Senators, including Senators Sununu, Durbin, Murkowski, Salazar, Hagel, and others. This bill places new safeguards on the use of national security letters and related PATRIOT Act authorities to protect against abuse and ensure the constitutionality of the statute.

Among other things, it restricts the type of records that can be obtained without a court order to those that are the least sensitive and private, and it ensures that the FBI can only use NSLs to obtain information about individuals that have at least some nexus to a suspected terrorist or spy. I am pleased that it has received endorsements from all over the political spectrum, from the Center for American Progress, to the League of Women Voters, to Grover Norquist of Americans For Tax Reform.

I would ask, Mr. Chairman, that an April 22 letter in support of the bill, as well as a "Dear Colleague" about the bill, be included in the record.

Chairman LEAHY. Without objection, so ordered.

[The prepared statement of Senator Feingold, with attachments, appears as a submission for the record.]

Senator FEINGOLD. Thank you, Mr. Chairman.

This legislation is a measured, reasonable response to a serious problem. Again, thank you very much for holding the hearing on the bill and on this topic, and I look forward to the witnesses' testimony.

Chairman LEAHY. Thank you.

Senator Cardin, did you wish to—

STATEMENT OF HON. BENJAMIN L. CARDIN, A U.S. SENATOR FROM THE STATE OF MARYLAND

Senator CARDIN. Thank you, Mr. Chairman. Just very briefly, let me first comment that I will be moving between this Committee and the Foreign Relations Committee that has a hearing on Darfur today. I'm saying that for Senator Specter's benefit, because I'm sure his colleagues are very busy in other committees that are holding hearings today.

But obviously this is an extremely important hearing, and I thank you very much for conducting this hearing.

I just want to make a quick observation, if I might. I think Americans would be very surprised to learn that there are tens of thousands of national security letters issued every year—every year—the majority of which are directed toward Americans, requesting sensitive information such as their credit information or their telephone records, and it is done without any court supervision. They also, I think, would be surprised to learn about the In-

spector General's report that pointed out that a large number of these letters were issued contrary to the law, in violation of the authority that the Department had.

So I think it's very important for us to do the appropriate oversight. I'm sure we're going to hear today, Mr. Chairman, that as a result of the Inspector General's report, as a result of the oversight that this Committee has done, that the circumstances are improved, that procedures are now in place, that the number of violations of laws have been reduced dramatically and that the circumstances and the use of national security letters have improved dramatically.

But what happens when we turn off the spotlight? What happens when Congress does not hold regular oversight hearings on the use of national security letter? Will we revert back to the use of these letters, contrary to law? When one agency can make a decision without review of the courts, without oversight, there is the potential for abuse.

So I just want to compliment Senator Feingold for his legislation. I think it's important that we look at ways in which we can establish the appropriate check-and-balance in our system to make sure that the agencies have the tools that they need to protect our country and to pursue investigations that are important so they can get the material necessary for investigations, but at the same time protect the civil liberties of the people of our Nation. Clearly that was not done over the last five or 6 years. Clearly that was abused and did not further justice, and it did hurt the civil liberties of the people of our country.

So I think that we should not only be holding the oversight hearing that Senator Specter has talked about the importance of, but to look at ways in which we can institutionalize a better check-and-balance system on the use of this extraordinary power by the Department of Justice.

Mr. Chairman, I look forward to our witnesses. Again, I apologize if I have to leave to attend another hearing on the circumstances within the Darfur region of Sudan.

Chairman LEAHY. Thank you very much.

Senator Whitehouse, did you have anything you wanted to add?

STATEMENT OF HON. SHELDON WHITEHOUSE, A U.S. SENATOR FROM THE STATE OF RHODE ISLAND

Senator WHITEHOUSE. Thank you, Mr. Chairman.

Very briefly, I just wanted to commend Senator Feingold for his legislation. He has undertaken what those of us who have the honor of working with him have come to expect as a very thoughtful and thorough approach to this issue. I think we should also take a moment, if it has not been done already, to commend Inspector General Glen Fine. We are here, in large part, because of the research work that he did.

Our job is to oversee the executive branch and remark and bring attention to situations where folks have failed in their duties or failed in their responsibilities, and assure that those mistakes are cured. It is also, I think, our responsibility to express appreciation and pride when folks in the executive branch do their duties particularly well.

I think the Department of Justice Office of Inspector General did its duties particularly well in this respect, and I think the record of the hearing should reflect that. I remain a little bit dismayed that the FBI, as an institution—I had this discussion with Director Mueller when he was here—did not more highly value the rather extraordinary powers that they were given in this legislation and the responsibilities, the concomitant responsibilities that came with that.

The fact that there wasn't adequate internal oversight, that there weren't checks and balances going, frankly, right up to the Director's office, because this is an issue that directly affects the credibility of one of our proudest law enforcement agencies with this Congress, and if they're not minding the store when we give them the kind of scope—I think mistakenly, but irrespective of that—that they are and it's cabined with particular congressional restrictions, the level of disinterest in attending to those congressional limitations is kind of surprising.

You would have thought that the highest levels of the FBI, somebody would be saying, you know, this is pretty serious stuff, they put some pretty serious boundaries around it. We're going to look like real dopes if we foul this up. You know, somebody in my office is going to be in charge of making sure this is done right. The failure of that, I think, is an interesting and significant failure in this whole process.

So I very much look forward to the testimony of all the witnesses. I appreciate the Chairman holding this hearing, and I thank Senator Feingold for, once again, his thoughtful and thorough approach to an important issue.

Chairman LEAHY. Well, thank you very much.

Gentlemen, you've had a chance to hear our views on this. Don't let that influence you in any way, shape, or manner as you give your testimony. I mean that, seriously.

The first witness will be James Baker. He has an extensive background in the area of national security. He served at the Justice Department for 17 years. He was Counsel for Intelligence Policy in the Office of Intelligence Policy & Review from 2001 to 2007. Is that correct? A former Federal prosecutor, he's worked on a wide variety of national security matters. He taught national security law at Harvard Law School in 2007. He's a Fellow at the Institute of Politics at Harvard's Kennedy School of Government. He currently serves as the Assistant General Counsel for National Security at Verizon.

He received his bachelor's degree from the University of Notre Dame and his law degree from the University of Michigan Law School.

Mr. Baker, please go ahead, sir.

STATEMENT OF JAMES A. BAKER, FORMER COUNSEL FOR INTELLIGENCE POLICY, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. BAKER. Thank you, Mr. Chairman, Ranking Member Specter, and members of the Committee. I appreciate the opportunity to be here today.

Let me just say at the outset that I am appearing here today in my individual capacity at the request of the Committee and anything I say should not be taken as reflecting the views, necessarily, of my current or former employers.

So, Mr. Chairman, you have my written statement, which I would ask to be made part of the record.

Chairman LEAHY. Without objection, it will be part of the record.

Mr. BAKER. Thank you, sir.

[The prepared statement of Mr. Baker appears as a submission for the record.]

Mr. BAKER. I won't try to recapitulate what I say there, but my objective today is to try to be of whatever assistance I can to the Committee to try to put national security letters in context with what the intelligence community, the FBI, is doing every day to conduct national security investigations and to obtain foreign intelligence information. So what I am urging today is that we think about this in a holistic way and try to understand the perspective of the people on the ground who have to use these tools as they go about doing what everybody agrees we want them to do, which is to protect the country.

And so what I urge is we not focus just on NSLs, but we think in a larger way about the whole question of what I refer to as metadata. I'll come back to that. Well, I'll just address that right now.

Metadata, as I describe in my written statement, what I mean by that, and what other people have referred to or used that term to refer to, is really a distinction between content information and non-content information. Content information is the words that are spoken on a telephone call, the substance of an e-mail, what happens in the privacy of our homes, those kinds of things. That's the content that I refer to.

When I'm talking about metadata I'm talking about non-content. It's information about those things, maybe the date, the time, the duration of the telephone call, the "to" and "from" of an e-mail, indications about where you moved at different points in time, but it's not your actual substance of your communications.

So what I think, and what I'm trying to say today is that Congress, I suggest, should think about the problem or the issue of the collection of non-content information and how it wants the government to go about doing that, and what rules apply, what oversight there should be, and so on.

Metadata, generally speaking, is not protected by the Fourth Amendment. Content is protected by the Fourth Amendment. Metadata is protected in some instances by statute, but in many instances by nothing. There are no statutes with respect to certain types of metadata. So what I think Congress needs to think about, is what does it want the government to do? What do we as Americans want the government to do with respect to the collection of all types of metadata, from the types of metadata we're talking about today from national security letters, but broadly, all different types of metadata? That's the big issue. That's the big privacy issue, I think, that faces us today.

Let me just say, metadata is a critically important tool for conducting national security investigations. It's been referred to as the

bread and butter of FBI investigations. But I don't want to oversell it, either. It's not a panacea. It may be the bread and butter, but it's not necessarily the main course or the dessert. I mean, it's not everything. It provides you with certain guideposts and ways to think about problems and who to focus on, but it's an investigative tool, not an investigation.

My main criticism, I think, of the current statutes that we have, and I urge the Congress to think about it as it decides what to do next, is that they are just way too complex. There are too many tools that are out there for the government to use with too many different standards, too many different approval levels, too many different oversight mechanisms with respect to the collection of metadata.

For example, as I said in my written statement, there are eight different ways, by my count, at least, to get telephone toll records. There are eight different ways, with all kinds of different standards. That's too complex. That is what leads to, I think, some of the confusion that ensues that you see reflected in the Inspector General's report, which I also commend. I think it's an excellent report.

So I think as you consider what to do next, you should worry about making things too complex. That's what I urge you to worry about with respect to that. You should also worry about making sure there's adequate oversight. You should make sure that there are the right people in the right jobs, working hard to get it right. That's critically important. I also urge that there be adequate and statutorily mandated minimization procedures with respect to all different types of metadata. Senator Feingold's bill urges that, or would require that with respect to national security letters, but you need to think broadly and think about other types of metadata that are collected from a variety of different sources.

As I suggest in my written statement, one thing to think about would be a national security subpoena. It would be simple, it would be broad in scope. It wouldn't be unlimited in scope. It wouldn't be able to collect certain types of data if you wanted to restrict that, such as tax records and so on. It would not be an administrative subpoena, it would be a subpoena that would require the involvement of the Department of Justice.

I see my time has expired, Mr. Chairman, so I will stop there. But what I urge is, do not approve a national security subpoena unless you also provide for adequate oversight mechanisms, provide resources for that, and require minimization.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you. We will go into what you mean by adequate oversight on that.

The next witness is Gregory Nojeim—did I get that correct?

Mr. NOJEIM. Yes.

Chairman LEAHY. Thank you. He's a Senior Counsel and Director of the Project on Freedom, Security & Technology at the Center for Democracy & Technology in Washington. He's a recognized expert on Fourth Amendment and surveillance issues arising in the national security and intelligence areas. Before joining CDT in May of 2007, he was the Associate Director and Chief Legislative Counsel for the American Civil Liberties Union. He received his bach-

elor's degree from the University of Rochester and his law degree from the University of Virginia.

Go ahead, sir.

STATEMENT OF GREGORY T. NOJEIM, DIRECTOR, PROJECT ON FREEDOM, SECURITY & TECHNOLOGY, CENTER FOR DEMOCRACY & TECHNOLOGY, WASHINGTON, D.C.

Mr. NOJEIM. Thank you, Senator Leahy, Senator Specter, members of the Committee. Thank you for the opportunity to testify today on behalf of CDT.

The DOJ Inspector General found widespread errors and violations in the FBI's use of NSLs to obtain bank, credit, and communication records of U.S. citizens without prior judicial review. These violations are the natural, predictable outcome of the PATRIOT Act and other legal and technology changes. They weakened the rules under which FBI agents make these demands while dramatically expanding their scope. In response, the FBI issued detailed guidance on NSLs that contains many useful elements.

But internal reforms can only fix so much. The only way to truly address the problems is to legislate traditional checks and balances under which a judge must approve governmental access to sensitive information.

So far, NSL legislation has been a one-way street. With almost every change in the law, more records from more businesses with more personal information about people increasingly distant from the target of the investigation have been made available to more people in government, with more coercion and less judicial oversight. And, the judicial review that has been provided for has been largely toothless.

Self-policing doesn't work. Going to a judge makes a difference in a way that is unachievable by merely internal reviews or by reviews conducted by attorneys in a different part of the executive branch.

Senator Specter said, "Thank God for the courts." It's time to give the courts something meaningful to do in this context.

We ask that you enact legislation that reflects the principle that the more sensitive the information sought, the tighter the standard should be for getting it and the more exacting and detached the review for the request for information should be.

When revealing information is sought in an intelligence investigation, mere relevance without judicial review and without a tie between the subject of the records and a foreign power is an inappropriate standard. The weak relevance standard is often justified by drawing parallels between NSLs and criminal subpoenas, which are issued without prior judicial review.

But intelligence investigations are more dangerous to liberty than criminal investigations. They require stronger compensating protections.

Intelligence investigations are broader than criminal investigations. They are not limited by the criminal code. They can investigate legal activity, including First Amendment activity.

Intelligence investigations are conducted in much greater secrecy than criminal cases, even perpetual secrecy. When a person receives a grand jury subpoena, normally a person can complain

about it. In an intelligence case, when a business gets an NSL, they're gagged. They're prohibited by law from complaining about it, and the subject of the NSL never learns of it.

Finally, in a criminal investigation almost everything the government does is ultimately exposed to scrutiny. The prosecutor knows that at the end of the day, his actions will often come out in public. That is a powerful constraint. There's no public airing at the end of intelligence investigations.

In this context, the relevance standard offers insufficient protection against abuse. There is just no substitute for tightening the standard and subjecting requests for sensitive information to judicial review.

After-the-fact minimization, while it's important, doesn't prevent the initial intrusion. Minimization under FISA, the model that many urge for NSLs, is actually quite permissive.

Moreover, none of the changes that the FBI has put in place can get to the core issue. That is to ensure that NSLs are used only in a focused way when there is a factual basis for believing that the individual whose data is sought is a terrorist or a foreign agent, or that information is otherwise sufficiently important to the activities under investigation.

The NSL Reform Act, in contrast, does get to the core issue. It creatively honors the principle that sensitive information deserves more protection. First, it would separate information that can now be obtained with an NSL into sensitive and less-sensitive personal information.

Not all metadata is created alike. Some of it is particularly sensitive. The "to"/"from" information about a person's e-mailing is more sensitive than information that merely identifies a person.

Yesterday I applied for a loan at a bank. The records that I gave to the bank might be regarded as metadata under this proposal. I had to give them my tax return and a lot of other sensitive information that, frankly, I didn't want to give up, and frankly shouldn't be available to law enforcement without a really good reason.

We like the way that the NSL Reform Act separates out these two types of sensitive information to less sensitive and more sensitive, and says that when the information is more sensitive there has to be some judicial authorization, usually -probably -through Section 215 of the PATRIOT Act before the information can be given to the government. These are necessary reforms. They and other measures can ensure that the government has the tools it needs to prevent terrorism and that those tools are subjected to appropriate checks and balances.

Thank you very much.

Chairman LEAHY. Thank you very much.

[The prepared statement of Mr. Nojeim appears as a submission for the record.]

Chairman LEAHY. Our next witness, Michael Woods, is an attorney with extensive expertise in national security areas. He served in a variety of national security-related positions at the Justice Department, beginning his service in 1993. He served as Chief of the FBI's National Security Law Unit from 1997 to 2002. In private practice, he has advised Department of Defense clients in matters

of national security policy. He has published Law Review articles on national security law issues, including those related to national security letters and the PATRIOT Act. He graduated from the University of Oxford and Harvard Law School.

Mr. Woods, glad to have you here.

STATEMENT OF MICHAEL J. WOODS, FORMER CHIEF, NATIONAL SECURITY LAW UNIT, OFFICE OF THE GENERAL COUNSEL, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, D.C.

Mr. WOODS. Thank you, Mr. Chairman.

Mr. Chairman and members of the Committee, I am very pleased to have the opportunity to appear this morning. I think, really, I have two things to offer the Committee in this very important work. The first, is my practical experience. As a former Chief of the FBI's National Security Law Unit, I was basically in charge of the national security letter production process during the time I was there. I would add and would underline that I left the FBI in 2002, and so I am probably not the person who can comment on what has gone on more recently than that internally, or about the measures that have taken place.

But I can certainly give some insight into how these letters were used investigatively prior to the PATRIOT Act, into the rationale for the changes that were sought in the PATRIOT Act, and into some of the investigative concerns that I think persist to this day.

The second, of course, as the Chairman has noted, I have written on what I call transactional data, which Mr. Baker is referring to as metadata. I will use whatever term the Committee wants. I do not mean to create confusion. I have summarized this research in my written testimony, and I have appended a Law Review article that I think might be helpful.

Chairman LEAHY. Incidentally, all the written testimony of all the witnesses will be put in the record in total.

Mr. WOODS. Thank you, Mr. Chairman.

Like the other witnesses this morning, and I'm sure everyone on the Committee, I see in this constantly evolving digital environment an enormous challenge for our government. The cloud of transactional information or metadata that each of us now creates in our daily lives, though it may not contain the direct content of our private communications, reveals a steadily more detailed picture of our activities, our personal habits, our social networks, our finances. This information largely resides in the custody of third parties, in quantities, formats, and conditions of which most of us remain unaware.

The constant expansion in the capacity of digital storage systems and in the power of search engine technology make this transactional information at once more permanent and more easily accessible than ever before. This situation poses a real challenge to counterintelligence and counterterrorism investigators. On the one hand, it allows a new window into the hidden activities of our most sophisticated adversaries. On the other, the compromise of privacy by the acquisition of transactional data seems much greater now, that the quantity and detail of that information has increased.

I believe it is critically important that the Committee leave the FBI with a flexible and effective tool for obtaining transactional information. That tool should incorporate safeguards that inspire public confidence, but safeguards that are proportionate and carefully tailored in response to the actual harms.

Though I disagree based on my experience with the suggestion that the legal standard for national security should be returned to its pre-PATRIOT Act level, I think many parts of the current legislative proposal represent very promising steps in the right direction.

I am very happy to elaborate on these views in response to your questions, and look forward to assisting the Committee in this important work.

Again, thank you for inviting me.

Chairman LEAHY. Thank you very much, Mr. Woods.

[The prepared statement of Mr. Woods appears as a submission for the record.]

Chairman LEAHY. Over the last several years, the FBI issued virtually no guidance. They had no real checks or oversight on the expanded use of national security letters. We have had several Inspector General reviews which came about because Congress, in its oversight, insist on these reviews. They pointed out errors in every single aspect of the national security letters: they're drafted incorrectly; they're issued without even the minimal administration requirements; their use was not monitored; the information collected is often not even recorded or tracked.

So, in other words, these Inspector General reports showed that the FBI failed in every respect to police its use of NSLs. It was only after these devastating IG reports came out that the FBI took steps to control use, and then started issuing guidance, creating a data bank, and so forth.

But even now the FBI resists any process for outside review. Even though they had this abysmal record following on them, they don't want any outside approval. One article likens this to the stereotypical male driver who has circled the same block four times, but still stubbornly refuses to ask anyone for directions. My wife would like that one.

Now, haven't we seen enough from these IG reports? Though the FBI can't effectively check it's own use of this very powerful authority, do we have to wait for more years, and documents, and so on or should Congress require approval of the NSLs outside of the FBI? Who should be the reviewing authority? Should we have judicial review? You have differing views.

Mr. Baker, let me begin with you, then go to Mr. Nojeim, then Mr. Woods.

Mr. BAKER. Thank you, Mr. Chairman. Yes. I mean, I subscribe to the notion that it's appropriate to have review of metadata collection tools, whatever legal tool Congress ends up approving outside of the FBI. I think it's appropriate. I think it works well when you think about it in the criminal context or the grand jury process where the FBI agents need to go—must go—to a Federal prosecutor to obtain approval to issue the grand jury subpoena so there's an outside check on what happens before the document goes

out that results in the collection of the information. So, I think that's very appropriate.

I think that system has worked well with respect to grand juries. The difficult thing for the Committee is to try to calibrate what it does with respect to what the effect is. So the higher you ratchet up the approval levels, if you indeed require the FBI to go to a court in addition to a Justice Department attorney, it's just going to make it that much more difficult and that much more time-consuming to obtain the information. It will be something that discourages the FBI from actually trying to pursue those.

Now, some people say that's a good idea, we don't want them to do all these NSLs. But the volume, as you can see, of the number of NSLs is so huge and the time pressure is so great, that we need to have something that's—

Chairman LEAHY. But even now they're not even going to the U.S. Attorney.

Mr. BAKER. No, I agree. But with the NSLs, they just do it internally. It goes to the SAC, Special Attorney in Charge.

Chairman LEAHY. But you would not support judicial review because of the volume?

Mr. BAKER. For much of the information, I think judicial review is too much. I concede and think it would be a good idea if Congress wanted to carve out a certain set of records—tax return records, firearms records, educational records, the sort of things that are listed in the current 215—out and say, if you're going to have this category of material you have to go to the court. But for the transaction, for much of the transactional data, again, I agree with Mr. Woods, we need to be very careful. It needs to be carefully calibrated. You need to think about what categories you want to carve out and make sure they're really important.

Chairman LEAHY. Mr. Nojeim?

Mr. NOJEIM. That is exactly what the Feingold bill does. It carves out the more sensitive information and says for that tax return that was given to the bank so a person can get a loan, for e-mail "to"/"from" information, you've got to go to a court first. It's not good enough for the FBI to check itself.

Let me just say a word about the checks and balances that we're calling for. One doesn't normally think of a person in the executive branch charged with being a prosecutor or protecting national security as being the person who provides the check and the balance. It's the judge who has to provide that check and the balance. That's their role in our system. It's just not the proper role of prosecutors to be actually charged with that. They can certainly help, but a true check has to be judicial.

Chairman LEAHY. And Mr. Woods?

Mr. WOODS. I guess I would agree with the idea that there needs to be judicial review available, but I would focus directly on the calibration. I would draw the analogy to the grand jury. The former prosecutors on the Committee know that, as a prosecutor, you might issue hundreds of grand jury subpoenas. Now, the possibility of judicial review is there, but it's the prior approval of the court, and in most instances in the Federal system, prior approval of a grand jury is not something that is required. I think we have to shift toward that analysis.

Chairman LEAHY. Of course, in the grand jury the prosecutor eventually is going to have to answer to the court how he collected the evidence.

Mr. WOODS. Exactly.

Chairman LEAHY. They're not going to say, OK, on every one of these subpoenas you have to have a witness come in, but at some point they're going to say, it appears you overreached, or you didn't. Is that not correct?

Mr. WOODS. That is correct. But I think that one of the things we'll certainly end up discussing here is the very fundamental distinction between the collection of intelligence and criminal investigations. I mean, Congress and the executive branch have struggled with the oversight of these activities for a long time because that public accounting is not present in the intelligence world.

Chairman LEAHY. Thank you.

Senator Specter?

Senator SPECTER. Thank you, Mr. Chairman.

Mr. Baker, in my opening statement I referred to a situation where the FBI had been twice turned down by the FISA court on a request for a Section 215 order for business records and they then used a national security letter. I am advised, further, that at the time you were head of the Office of Intelligence, Policy & Review in the Department of Justice and that you advised the FBI that they ought not to use a national security letter in that context. Is all of that true?

Mr. BAKER. It is true, Senator, that I was head of the Office of Intelligence & Policy Review at that time. Senator, I don't recall, sitting here today, giving that advice with respect to NSLs.

Senator SPECTER. Do you recall the situation where the FBI had twice been turned down by the FISA court for a Section 215 order?

Mr. BAKER. I remember the case in general, Senator. I would just comment, just as a point of clarification—and I can talk more about how the FISA process works—but it was—

Senator SPECTER. Well, I don't have much time. There was such a case. Then the FBI did use a national security letter in that situation?

Mr. BAKER. With respect to that investigation, yes.

Senator SPECTER. Well, that's pretty blatantly wrong, isn't it, Mr. Baker?

Mr. BAKER. Well, technically speaking, under the law they were authorized to do it. Now, that doesn't mean necessarily that it was a good idea to do it with respect to the facts that are here in this case.

Senator SPECTER. Well, did the court turn it down because there was a First Amendment issue?

Mr. BAKER. My understanding is that the court did not officially turn it down. There was a back-and-forth between the government on a number of—

Senator SPECTER. OK. But the court didn't grant it?

Mr. BAKER. I beg your pardon?

Senator SPECTER. The court didn't grant it.

Mr. BAKER. I'm sorry. I didn't—

Senator SPECTER. The court didn't authorize the order?

Mr. BAKER. No, it did not, sir.

Senator SPECTER. OK. Well, with 5 minutes of talk, that's enough on this issue. To me it's pretty plain that the FBI is circumventing the court, which had it twice before it. It wasn't granted. That's the critical aspect.

Let me move to you, Mr. Nojeim. You call for "specific and articulatable facts" for NSLs. Others have contended that the relevance standard is sufficient. Isn't a standard of relevance, which is not even reviewed by an attorney, highly subjective and highly questionable just on the say-so of an FBI agent?

Mr. NOJEIM. It is. It is. One of the problems with a relevance standard—

Senator SPECTER. Would it slow down the process to make it impractical if your standard of a specific and articulatable facts standard were to be required?

Mr. NOJEIM. No, I don't think so. The FBI guidance actually requires agents now to articulate the reasons why they believe that the information sought is relevant to the investigation.

Senator SPECTER. Mr. Woods, what do you think about a "specific and articulable facts" standard for NSLs?

Mr. WOODS. I think it's inappropriate.

Senator SPECTER. You think what?

Mr. WOODS. I think it's inappropriate. I believe it's inappropriate because it was the standard prior to the PATRIOT Act. It did slow the process prior to the PATRIOT Act and it did make these tools far less available.

Senator SPECTER. Well, was it a good process? Just being part of the PATRIOT Act doesn't speak to its value, speak to its appropriateness.

Mr. WOODS. As I've outlined in my written testimony, it was a process and a standard that worked very well in the traditional counterintelligence cases of the FBI in chasing spies, in cases where you make fairly common investigative links from known agents out to their associates, et cetera.

It did not work very well in the kind of inchoate threat situations that we were encountering in terrorism where you don't have a lot of facts about the individual, therefore you don't have specific facts about the person to whom you are trying to connect. This is where that standard started to break down in the 1990's, and it's why the FBI asked for it to be changed.

Senator SPECTER. Mr. Woods, what do you think of Judge Posner's argument, which was made again in March of 2007 in the Wall Street Journal that the FBI, really, institutionally, is not the best agency to handle this, going again and looking to the idea of a United States Mi–5. What do you think of that?

Mr. WOODS. I've never been in favor of that. I disagree with Judge Posner on that, and some other things.

I actually think it is a good—I mean, the critics like Judge Posner say that it's the FBI's investigative criminal orientation that slows down the intelligence gathering process. I think that if you're going to have anyone do domestic intelligence collection, and I think someone needs to, it ought to be people who are steeped in the criminal process, in the constitutional process rather than the kind of people we have collecting foreign intelligence, for example, who lack that background.

Senator SPECTER. Thank you very much.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you, Senator Specter.

Senator Feingold?

Senator FEINGOLD. Thank you, Mr. Chairman.

Mr. Baker and Mr. Woods, according to the Inspector General's reports the FBI uploads information it obtains through NSLs into numerous data bases that are widely accessible to tens of thousands of personnel at the FBI and other agencies.

I'd like to ask you both, should all this information be retained indefinitely, and what type of limit should the FBI be required to impose on the type of information it retains and the length of time it is kept?

Mr. Baker?

Mr. BAKER. Well, as I have said in my written statement, Senator Feingold, I think there should be rules. There need to be minimization rules. As your bill would require for national security letters, I would urge you to require it for all types of metadata. It's something that Congress needs to worry about, not just with respect to the fruits of the national security letters, but with respect to all the types of data from all the different tools that the government uses to collect metadata, including grand jury subpoenas, pen register trap and trace orders, all kinds of things.

That said, with respect to destruction, I do say in my statement that I think, if you're going to allow the government to collect a lot of data on the front end, you need to minimize the retention and dissemination, and at some point in time it needs to be destroyed.

Senator FEINGOLD. Well, the FBI would probably argue that you can never predict when the information might be useful. Based on your government experience, how quickly does the utility of this type of information as actionable intelligence start to decrease? I realize you can't say an absolute answer, but what is your sense as a professional in this area?

Mr. BAKER. If you're trying to get actionable intelligence which will allow you to actually do something to stop a threat, stop a spy, it starts to dwindle relatively quickly. So what I suggest in my testimony is a pretty long time period, which is 5 years, destruction after 5 years.

You can come up with examples where 10, 15, 20 years would reveal something about someone, but it is—I don't know how you want to say it, but it's a slope that drops pretty quickly, Senator. So I think definitely after 5 years, and at some point even before that it drops off quickly.

Senator FEINGOLD. Thank you, Mr. Baker.

Your response to this issue, Mr. Woods?

Mr. WOODS. I think, definitely, there needs to be a mechanism for governing the retention of this information. The national security letter statutes were developed kind of quickly. They've been ignored and in a corner for most of their life. It's really a mistake that these statutes didn't have something like this from the beginning. And I would agree with Mr. Baker. I think for a model we would look at other things, the retention rules that we put in the Attorney General guidelines, the retention rules that are in the

DoD guidelines. There should be that kind of review to eliminate retention as quickly as possible.

Senator FEINGOLD. Based on those responses, I'd like to ask each of the witnesses if you could give a "yes" or "no" answer. Is it safe to assume that all the witnesses support the provision of the NSL Reform Act mandating that the FBI issue minimization and retention procedures for NSLs?

Mr. Baker?

Mr. BAKER. Yes, I do. But I would also suggest that you should worry about acquisition, minimization at the stage of acquisition. Don't get more than you really need for the purpose that you're searching for it.

Senator FEINGOLD. Mr. Nojeim?

Mr. NOJEIM. Yes, I agree.

Senator FEINGOLD. OK.

Mr. Woods?

Mr. WOODS. Yes, I agree, too.

Senator FEINGOLD. And I want to thank the Ranking Member for raising the issue of the relevance standard, which I consider, of course, to be woefully inadequate to protect the privacy of Americans who have done nothing wrong. I believe that the specific and articulable facts standard is an appropriate standard, but we will certainly work on this legislation to make sure that the government can get what it needs, but not go too far.

I do think that the relevance standard is not adequate, and as Senator Specter said, the mere fact that it was put in as a change in the PATRIOT Act is not to me, a recommendation. It is actually a sign that it might not have been looked at closely enough, because that's my view of the whole legislation.

Mr. Nojeim, the most recent Inspector General report indicated that the percentage of NSL requests generated in the course of investigations of U.S. persons has increased steadily in the past several years, from 39 percent in 2003 to 57 percent in 2006. Is this cause for concern?

Mr. NOJEIM. Yes, it is. I think that you can trace that increase to the PATRIOT Act itself, which eliminated the requirement that the records pertain to an agent or a foreign power. Most Americans don't fit that description.

Senator FEINGOLD. And also, Mr. Nojeim, the FBI conducted its own internal review of 10 percent of all NSLs issued from 2003 to 2006. According to the most recent Inspector General report, the FBI's review found more than 550 instances in which the FBI received records it had not requested in response to an NSL, yet out of those hundreds of incidents only four times did the FBI realize that this violation had occurred. That's less than 1 percent. The IG report also stated that at least some of this unlawfully obtained information was uploaded into an FBI data base that is shared more widely with the intelligence community. What does that tell us about the extent to which these data bases may contain unlawfully obtained information?

Mr. NOJEIM. It suggests that there could be a big, big problem. We won't know what information in the data base was lawfully obtained and what information wasn't. It's not tagged, so you just won't know.

Senator FEINGOLD. Thanks to all the witnesses.

Thank you, Mr. Chairman.

Senator WHITEHOUSE. Thank you.

I believe Senator Sessions is next in order.

Senator SESSIONS. Well, I think the FBI deserves criticism for not managing this program well, not following strictly the guidelines and accounting correctly in the beginning. Wouldn't you agree, Mr. Woods?

Mr. WOODS. Yes, I would.

Senator SESSIONS. And Mr. Mueller came here and promised to do better, and the OIG report indicates that they have done better and fixed the problem in recent months. Is that correct?

Mr. WOODS. That's the testimony.

Senator SESSIONS. I think we heard—we know what happened. We saw the Director in here. This oversight Committee, which has the responsibility to make sure this program is going right, we grilled Mr. Mueller, we made him promise to do better, and he's done better.

Now, let me ask you this, Mr. Woods. Isn't it true that a DEA agent investigating an American citizen can issue a subpoena for some person's telephone toll records if he thinks it's relevant to a drug-dealing operation?

Mr. WOODS. That is absolutely true.

Senator SESSIONS. And IRS can get your bank records if they think you may be cheating on your income tax.

Mr. WOODS. That's correct. There are actually over 300 Federal agencies that have administrative subpoena authority that is based on the relevance standard.

Senator SESSIONS. And Mr. Nojeim, forgive me if I object, but I do not believe, and strongly reject the idea that we ought to give greater protection to terrorists and spies than we give to drug dealers and tax cheats. I just do not believe that's accurate, and fundamentally that is what I understood you to be saying.

Mr. NOJEIM. What I have said, Senator, is that intelligence investigations are different. If you're conducting a criminal investigation of a terrorist who may have committed a crime or a spy who may have committed espionage, which is a crime, the same rules apply. What we're talking about is a different kind of investigation, one untethered from a criminal charge or from criminal suspicion.

Senator SESSIONS. Well, OK. Now, Senator Specter asked the question about specific and articulable facts, shouldn't that be the standard. Well, Mr. Woods, isn't it true that DEA doesn't have to quote articulable facts to get your telephone toll records?

Mr. WOODS. That's correct.

Senator SESSIONS. Or the bank records.

Mr. WOODS. No. These—

Senator SESSIONS. Or your motel records.

Mr. WOODS. All of these transactional records are basically available in the other context, criminal, administrative subpoenas, on relevance to the investigation, Senator.

Senator SESSIONS. So we absolutely ought not to be adding greater difficulties for investigators investigating a life-and-death situation, perhaps, than we do for drug dealers. And let's make this clear, Mr. Baker. You're a lawyer, and all of this. But the reason

is, these are not the individual's records. These are records in the possession of a third party. They have a diminished right of privacy in those records because they're not their records. You can't subpoena an individual's home computer. You can't subpoena their personal records and obtain those records without a warrant, if they object. But you can subpoena records at the Office of Motor Vehicles, at the telephone records or bank records, right?

Mr. WOODS. That's correct. The Fourth Amendment protects things with respect to which you have an expectation of privacy, and the type of things we're talking about today, the transactional data, is not protected by the Fourth Amendment.

Senator SESSIONS. And every day in America, Mr. Woods, every county attorney in America investigating any kind of misdemeanor or offense that wants records can issue a subpoena based on the standard of relevance to that investigation in every State in America that I know of. Would you agree?

Mr. WOODS. Yes, I would.

Senator SESSIONS. And since time immemorial, that's been the standard that prosecutors have used.

Mr. WOODS. Yes.

Senator SESSIONS. And how we're in this deal where we want to put more standards, more burdens on people who are trying to protect the American people from an attack is beyond my comprehension, and I'd object to it.

Let me ask this, Mr. Woods. Let's say you're investigating a person that you think may be connected to—you have some indication they may be connected to Al Qaeda and you issue a subpoena on the relevance to the investigation and get those telephone toll records. You see a lot of other calls to someone else and you want to now subpoena that person's records to see if they may have—see what connections those phone numbers show.

Now, in this context there may not be anything. It may be a perfectly innocent series of phone records you receive. But isn't it possible, and isn't it what we pay our investigators to do, if lo and behold there's a call to some known Al Qaeda number in Iraq or Afghanistan? Isn't that what we're about?

Mr. WOODS. Well, yes. I mean, that's the goal of these investigations, along with the goal of eliminating the people who are not, which is another function of these types of legal authorities.

Senator SESSIONS. Well, I don't know if somebody got my phone—my time is up. We also need to be sure that the information we're obtaining is not the power to listen in on these phone calls, but it's just simply the telephone toll records that show where that person may have called in the past. Is that correct?

Mr. WOODS. That is correct. These national security letters do not get content of phone conversations or e-mail content.

Senator SESSIONS. And I would point out that we tightened these standards when we reauthorized the PATRIOT Act. I didn't think they needed to be tightened, but we tightened them, all to make sure that spies and terrorists have their full rights—in fact, more rights than we give the drug dealers in America.

Senator WHITEHOUSE. Senator Kyl? While I am chairing, I am going to be the last person here, I'm very happy to have you go

ahead, if you would like to. I'd be happy to defer to you at this point.

Senator KYL. I am going to be here for a while, so please go ahead.

Senator WHITEHOUSE. Thank you.

This is, I think, a very, very interesting question that we have and it's a very interesting hearing. I see it in a slightly different context than Senator Sessions does, although we share the experience of both having been prosecutors and U.S. Attorneys.

It strikes me that there is a privacy interest that is raised that is separate from the privacy interest or value of a particular piece of data once you start to multiply and aggregate it into an enormous pool of data. It's something we don't have much guidance on from the Constitution, because at the time the Constitution was written the way an investigation worked was, the marshall or the sheriff came to your house, seized whatever evidence was necessary, brought it before the prosecutor or the magistrate, whoever, and when it was done, whether it was a bloody axe, a contract document, or whatever, it was either contraband, in which case it was destroyed, or it was of no value, in which case it was discarded, or it was returned and that was the end of that.

Then along comes the Xerox machine. Now documents start to live on in the files of government agencies. Fortunately—or unfortunately—they are paper files. They're very hard to go back and search.

So while they're still there for somebody who remembers, you know, in the so and so investigation I think we did this, let's go back and see what we found when we searched Joe Smith's house, we still have that in that file in this paper record, it's not a very live record.

Now, electronically we can not only preserve it, but we can aggregate it and we can maintain it indefinitely, and we can build, in theory, a massive consolidated data base of all of this information that people could plow through at will.

I do think, despite the fact that none of those individual pieces of data might rise over Fourth Amendment levels, it does raise a new question that we as a society need to address. So I would ask you to comment a little bit on those thoughts, and in particular the sort of nexus or matrix between the intensity of the privacy value of a particular piece of data that is sought versus the intensity of the investigation itself.

I am not sure whether I would be more concerned as a citizen about my privacy if the government said, look, I want 1 year's tax records for this one purpose or if they said, every phone call you have ever made, we are going to track who you made it to, when you made it, when it ended, and we're going to share it with all people who are interested.

The privacy balance, I just think isn't that easy, yet it's hard to measure that intensity of government investigation component. It's so much easier when the document itself is the trigger. How would you recommend—do you have thoughts on how you'd recommend we cope with that concern? And I'll followup further.

Mr. BAKER. Senator, at the end of my written statement I have a statement in there about, as time goes by—you're exactly right—

and our data collection capabilities increase, every human endeavor that can be reduced to a digital form will be collected by someone for some purpose, either commercially or for intelligence purposes or law enforcement. That's the direction we're heading in. These do become extremely powerful tools. They're powerful tools to protect the country. They're powerful tools that, when you have an urgent situation, you can go into a data base, you can search through, you can look for connections.

Senator WHITEHOUSE. And they're valuable tools. They're important tools, I think we all agree.

Mr. BAKER. Right. Extremely valuable.

Senator WHITEHOUSE. But they still need some—

Mr. BAKER. They need oversight. They need oversight and they need minimization. They need oversight by people. We can have all of our technology, we can have all of our systems, we can have all of our laws, quite frankly, but at a certain point in time the people matter.

For example, it mattered that Glen Fine was Inspector General at the Department of Justice at the time that you ordered a review of these things. I've worked with Glen closely and he's a very tenacious, intelligent, hard-working person. It mattered who he was. So you really have to make sure you have the right people in those jobs, doing the right thing.

At a certain point—I know time is almost up—you are right, I think, to focus on the Fourth Amendment issues. At a certain point in time, when the government's knowledge about our activities becomes so pervasive, that may, in fact, raise Fourth Amendment concerns. I think it's something that we're going to be struggling with.

Senator WHITEHOUSE. Let me interrupt you now, because my time has expired and I do have plenty of time with you once Senator Kyl has a chance to ask his questions, and yield to the distinguished Senator.

Senator KYL. Thank you very much. I think we all agree that, over time, the challenge presented by the acquisition of this transactional information is going to require us to develop new regimes or protocols of dealing with it.

What I'd like to do, especially with regard to how long you keep it, I do suspect that the last thing government agencies are going to want are roomfuls of data that they can't do anything with because they're simply too massive.

But what I'd like to do here is focus just a little bit on how this process actually works, the typical situation, because it gets to the standard that we're debating here and the reason why we went to a relevance standard.

This is transactional information about which the individuals had no expectation of privacy. Mr. Woods, you had experience in actually doing this and actually supervising it. Give us an example of how it worked. I'm specifically interested in why it's different in the context of preventing a crime from being committed, a terrorist act, as opposed to investigating a crime that has been committed.

Mr. WOODS. OK. I think that probably the best example is the sort of classic terrorist threat scenario that we run into a lot these days, where there is information, perhaps from foreign intelligence,

which indicates maybe a particular target or a particular city or a particular—there's been a foreign communication that is suspect. We don't know who made the communication, but it has enough characteristics that we're concerned about it and it says something about Washington, DC.

This is thrown to the FBI in a proactive mode. What can the FBI do? Well, the FBI could say—say it's sort of an e-mail, or the FBI might want to look at other e-mails that had connected to the same source, maybe it's from an internet cafe or something like that, and just do a quick scan to see, is this point of communication been in contact with anybody else that we know about, anything that might give us a lead? That transactional information about those communications is certainly relevant to the threat. It would be, I think, impossible in those situations to make out a specific and articulable facts case.

We don't know who the person on the other end of the communication is. We don't know for sure that they're an agent of a foreign power. It becomes very gray and circumstantial. We could spend a lot of time trying to work with that standard. That's kind of—I mean, that is why we asked, in the Bureau, for the relevance standard. There are situations where, you know, when the FBI is being mandated to be proactive and to depart from the investigative model, it's encountering these situations that don't fall into line with the standard that was designed for an investigative model. It is more dangerous. It is more risky in terms of civil liberties, but it is, in my view, what needs to be done now.

I would focus, therefore, more on the oversight, retention, and minimization end of this than on the legal standard itself.

Senator KYL. Now, that is the precise thing that I think we need to focus on. Why would you do that? Why would you want to retain the relevancy standard rather than going back to the articulable facts standard that we discussed earlier? Why would minimization procedures or other oversight be a better answer to the privacy concerns?

Mr. WOODS. Well, I think the standard itself, the scenario that I laid out, I think is going to become more and more common. We're going to need to assess threats quickly. We're going to need to respond to them quickly. But by their very nature, many of them are going to fall into the sort of fuzzy environment that the relevance standard is far better for. I mean, there's a reason why it's the standard for criminal investigations. This is how you quickly figure out what's going on.

I do think, though, where the system is breaking down is, once that's done, once that information is collected, how long do we keep it? What impulse is there for the government to sort through that? If I might, just one sort of side issue on this. The government—the FBI and other agencies—are facing two pressures. I mean, one is, get out there in front of the threats.

The other pressure is, share information. These data bases didn't exist when I was first in the FBI. They exist now because of our examination of the failure of information sharing prior to 9/11. So I think with those two things together, you need to reinvigorate the rules on minimization and retention. They were never added to national security letter statutes in the first place. All these things

came into existence without those, very unlike, say, FISA or criminal statutes in that regard. But that is why I would focus the attention there.

Senator WHITEHOUSE. Senator, can I just followup on that? Since it's down to just the two of us, we can be off the clock.

Senator KYL. Sure. That's fine. Go on, please. Senator Feingold might object to that now, but it's fine with me.

Senator WHITEHOUSE. Continue as long as you please, though.

Senator KYL. No. Let's just go ahead and have others respond to that if they like, and then a final comment. That will be fine.

Mr. NOJEIM. Mr. Woods has made a good case for the relevance standard, but the problem that we see with it is that it really doesn't have a good articulable end.

Say, for example, the threat information that is received is that there's a terrorist in Washington, DC. What information is relevant to investigating that threat? Is information about everyone who is staying at a hotel in Washington relevant? Is information about everyone who rented a car in Washington relevant? It just seems like there's no end.

Once you decide that information about who that person has communicated with is relevant, is information about who they communicated with also relevant, and so on, and so forth? So I guess the problem with the relevance standard is that it seems to untethered in that when we're talking about an intelligence investigation that is, again, not tied to the investigation of a particular crime, it seems like there's just no end to the information that could be obtained.

Senator KYL. I appreciate that point. But it seems to me that it, in some respects, ignores realities of life. That is, you've got some people who we have a lot of confidence in, we've given a great deal of authority to, to protect us from terrorism. We have put them into that position and they're in real-time situations trying to sort through a lot of material to be able to track something to get to the point where they can maybe stop a terrorist act from occurring.

They don't have time in that context, it seems to me, to sit around saying, oh, look at this juicy bit of information, let's set that aside and maybe we can deal with that later and really embarrass this political figure, or why don't we stop what we're doing here and gather up all this information for some other purpose?

I mean, they're on the tail of something, they're trying to get through it quickly. It seems to me that the problem is really quite the other way, and that is to be able to barrel through a whole of information as quickly as possible and not go back to what they just went through because it's of no immediate use to them, and they've simply got too much work to do to figure out what the terrorist attack might be to sit around and focus on all that.

So I think that the realities, the practical realities don't suggest that the problem is a likely big problem. I think, though, that ultimately there's got to be some decision made about, OK, now that's over did all of that stuff get captured someplace or did we simply go through it and it's simply out there in the ether again? To the extent we did make a record of some of it, what should be done with it?

I mean, I can see why privacy concerns there would require some mitigation or some procedures and protocols and so on. But during the process of trying to prevent the crime or the terrorist act itself, it seems to me that the broader standard giving them more flexibility and leeway to protect us is the appropriate way to approach it. That's my own point of view which I believe is pretty consistent with Mr. Woods'.

Senator WHITEHOUSE. The Senator from Wisconsin?

Senator FEINGOLD. Thank you, Mr. Chairman.

Let me briefly respond to what Senator Sessions, and to some extent Senator Kyl, said about the standard for getting an NSL. Senator Sessions mentioned grand jury subpoenas, which of course are to investigate crimes.

I believe that Congress should change the current relevance standard for NSLs. Intelligence investigations are not, as has been pointed out, subject to the same built-in checks that are present in criminal investigations. They are much broader, meaning that virtually anything could be relevant to an intelligence investigation. They are conducted entirely in secret. Investigative techniques are rarely tested through the adversary judicial process. I think that is why more oversight is needed, and that is why a more targeted standard is needed for the NSL authority.

So in that connection I would like to ask Mr. Nojeim, we have heard a proposal today for a new national security subpoena authority. Would you please address your thoughts on that proposal?

Mr. NOJEIM. I think that if the response to the Inspector General's reports is that there be a broader collection device—and that's what these subpoenas would be—that it's exactly the wrong response.

It's not clear to me who could receive one of these subpoenas. It does seem to me that they could be received by anyone as opposed to just the limited entities that are now possible recipients of national security letters.

There was no discussion about the gag that would come with one of these subpoenas. I put those two together because I think about who might be a recipient. What we're talking about is expanding the class of people who might receive a demand from the FBI for information, but, the demand says that they can't disclose anything about that demand.

It could be served on any person. I just don't know how my mom would respond to that request. I don't know how other people would respond to that request. I don't think that we should go in that direction as a result of the abuses that have been uncovered in the IG reports.

Senator FEINGOLD. I couldn't agree with you more. I can't imagine how granting the FBI administrative subpoena authority is a response to evidence of abuse of their current authority. We just barely dodged this bullet in the last round. For this to be a response to what we learned about the NSLs strikes me as kind of bizarre.

Mr. Nojeim, two Supreme Court decisions in the 1970s determined that Americans do not have Fourth Amendment rights to information they reveal to their phone companies or banks, such as the phone numbers they dial or the checks they write.

Given the unprecedented technological advances of the past 30 years, do you think these decisions would come out the same way again today?

Mr. NOJEIM. I think they're on shaky ground today. Take *Smith* v. *Maryland*, for example. That's the decision where the court decided that numbers dialed on a telephone didn't have Fourth Amendment protection. They reached that decision in part because those numbers dialed are not so revealing. The court said, for example, you can't even tell whether the telephone call was actually completed. You can't tell who was communicated with when those numbers were dialed.

Fast forward to today and think about the kinds of information that qualify as metadata, but that are much more revealing. E-mail "to"/"from" information. It's usually the case that you know who you're communicating with and the government will know when it gets that information. It knows the communication actually happened. So right there, it's much more revealing.

URL information—where a person went on the Internet. The closest parallel to that is probably library sign-out records, and most States protect those and require extra procedures. Yet, in the internet context, URL information, at least before the first backslash, is available with a national security letter.

Senator FEINGOLD. I commend all the witnesses for their testimony today. Mr. Nojeim, I particularly commend you for your ability today to distinguish not simply between metadata and content, but to point out that within the context of metadata there really need to be distinctions. It's not simply one kind of information or another, there are vast differences. You've done an excellent job of pointing out the dangers of not having those kind of distinctions within the metadata category.

Thank you, Mr. Chairman.

Senator WHITEHOUSE. Thank you.

I will sort of pick up where I left off, because I find this subject so intriguing. I think it's our next really big civil liberties issue to address. Does anyone dispute that it is essentially inevitable that, given the way we can electronically gather and store data, government data bases containing personal information are going to continue to proliferate and that, given the ease with which access to different electronic data bases can be increasingly achieved, there will be more and more access points for government agencies to those data bases? Are we not, to some degree, headed for a situation in which there is essentially a large, multi-accessed, multi-inputted, but essentially single government data base containing a vast amount of personal data related to American citizens?

Mr. BAKER. Senator, there may be a number of reasons you wouldn't want to create one data base, but you could have data bases that are linked in certain ways.

Senator WHITEHOUSE. Linkage makes it effectively the same, I think.

Mr. BAKER. It would allow you, with certain tools, to go through the different data bases. If your query fit the criteria for going into a data base, you could come up with some kind of a model to do that. So, I think that's right.

If I could just quickly respond to something that Senator Feingold said before he left, since it was my sort of bizarre idea to come up with this national security subpoena. Just, I want to be clear, and when Senator Kyl was talking about the different standards that apply, you can have relevance, you can have specific and articulable facts, you can have probable cause, but relevance, specific and articulable facts as to what? As to what? You have a twofold task in front of you. You have to pick the right standard, the right predication, how much facts you want to support it, but then as to what? You need to think about that.

My concern is, and the reason I came up with this bizarre idea—other people have too—is that if you raise the standard with respect to national security letters so high, FBI agents in the field will find some other way to get what they need because they are charged with, and have tremendous pressure on them, to prevent the next attack, as we all know.

So if national security letters are too difficult, well, let's see if we can find something else. 215? Oh, you've got to go to a judge. That's a pain in the neck; forget that. Oh. Grand jury subpoena? I'll just go to this AUSA that I work with all the time, we'll get that, and there's no court oversight in the real-time sense and you just get it from the AUSA. There's no minimization requirements. Boom, we've got it.

We've got the information that I believe I, the agent, need to protect the country and I'm not going to mess with these other statutes. So the volume will drop with respect to national security letters, it will be a less effective tool, but your insight into what is going on—your, the Congress' insight—the government's insight will just change. It will be harder to conduct oversight of those kinds of activities, and I urge that you worry about that.

Senator WHITEHOUSE. I understand that. But I think, in addition to the question you have raised of the "how do you get it" problem, we also have to address the "what do you with it" problem, which I think, as those of us familiar with this area—we would generally categorize that as the minimization problem. So you've got the "how do you get it" problem, then once you've got it, what do you do with it, how long can you keep it, do you destroy it, who can you connect to it, all that sort of stuff.

Then you have, as you mentioned, the predication problem, which is, who is allowed to query it. Who's allowed to hit the data base and under what circumstances? Is strikes me that if we're going to solve this problem we have to address really all of those three issues, that those are the three big prongs of this question from the government's point of view: what are you allowed to get, what are you allowed to do with it once you get it, and who are you allowed to let have a look at it, and on what terms?

Mr. NOJEIM. And to add just a couple more things. Not just what can you get, but what do you have to show to get it, and also what do you do with it after a few years? I mean, do you just throw it away or do you save it to see whether it might be useful in some other investigation 10 decades from now? I think that your—

Senator WHITEHOUSE. And minimization, I think, has become a hugely moving target. In my days as a U.S. Attorney, minimization basically meant that the agent flipped off the switch on the micro-

phone and stopped listening when it became apparent that the conversation was with the subject about pork chops for the weekend, that he'd called the butcher. Once you learned that this was an every Thursday call for Friday dinner, you didn't listen to it at all because you didn't any longer have a reasonable basis to listen to it. It was just kind of that simple.

Now, particularly in the FISA minimization context, it's gotten much more complex, much more deep in time, and into questions of distribution. So the simple ground rules very recently have had to adapt to a much more complex landscape, and I'm not sure that they're well understood.

Yes, Mr. Woods?

Mr. WOODS. Senator, there is a reason for that. That is—and we keep coming back to this matter of intelligence investigations—this is fundamentally different than the criminal context in that the adversaries we are facing are different. We are facing intelligence services with the full resources and backing of foreign governments. We are facing transnational terrorist groups.

So FISA minimization, for example, is structured after the fact, I think largely because of the language difficulties. You may be intercepting something on FISA that's in a dialect of, choose the language, and therefore the Congress allowed that to be done after the fact. I think we face the same thing here. To go to your earlier comments, it is important to remember that these intelligence investigations are not solely restrained by these statutes. We have 30 years of oversight, of regulation, of Attorney General guidelines, of executive orders.

The reason I put so much emphasis on retention/minimization issues is, over the years that has been the least-glamorous part of this work. I would say that minimization rules are stuck in the Xerox era, at best. What we need—I mean, minimization in the FBI, in my experience, was done with respect to FISA quite carefully, and one of the reasons is that every so often the Justice Department comes by and audits it. There's nothing like that. We've had national security letters since 1986. This is the first serious audit of how they are being used. I think, going forward, the Committee really ought to look at creating some of that, and at the same time maybe look at updating stuff from the Xerox era to something a little closer now.

Senator WHITEHOUSE. I also felt that the minimization process in Federal investigations that I oversaw, and at State investigations—I was a State Attorney General as well—was helped by the prospect that the Rhode Island State Police, local FBI agents, Secret Service agents, or ATF agents had that they were operating pursuant to an order allowing them to do this, which incorporated in its terms the legal requirement that they follow the minimization procedures, and that there was the prospect that a judge might at some point take an interest and say, you know, I signed this order and gave you the authority to collect this stuff, I told you you had to do it under these terms, I want to have a look. And just the prospect, I think, of judicial oversight was very helpful.

It's one of the reasons we've had this fight on the Foreign Intelligence Surveillance Act, because they put out minimization rules but they wouldn't let it be set up so that the FISA court ever had

the authority to see if they were being complied with, which completely undercut that motivation. I thought that was mistake, and thankfully I think we've corrected that in the FISA statute.

Mr. NOJEIM. I think that one of the reasons that we need the NSL Reform Act is that it requires that minimization procedures be adopted. There was a provision in the reauthorization legislation that required the Attorney General and the DNI to study whether minimization would be feasible. An NSL working group involving both agencies was put together. They recommended basically the FISA minimization procedures, but the Attorney General rejected that. I think it's time for you to say, we're going to have to step in and require that these minimization procedures be adopted.

Senator WHITEHOUSE. A lot of very sensible stuff seems to have been rejected for reasons that make absolutely no sense to me.

Senator Kyl?

Senator KYL. Well, let me just play off that point. There's a hierarchy of values here. One, is the protection of the American people from known dangerous enemies who have struck us with great destruction. We have instructed others in our government to see that that never happens again. Every one of us ought to be strongly committed to that.

Now, we also have the potential prospect of violations of privacy that might have an adverse consequence on someone, but I don't think there's a lot of evidence that that's happened yet.

I recall the words of the FBI agent who, about two and a half weeks before 9/11, complained to another that, because of the wall that separated two groups within the FBI, the Terrorist and Criminal Investigation, that someday somebody was going to get killed and then questions would be asked, and of course that's what happened.

So on the one hand, we have something that is critical for the protection of the American people, and we've seen breakdowns in that because we set up artificial legal barriers to the exchange of information and collection of information. On the other hand, we're all concerned about privacy because we can see in the future, if not today, a ballooning of information and access to information, and we're rightly concerned about how that's all used.

But I suggest we keep this in perspective, and that enabling the people to do the job to protect this starts with, I would argue, a lower standard like the relevancy kind of standard. Then in order to prevent that other potential from occurring, you can build on it. All of you have addressed that in one way or another, and I think we're all in agreement that both of those require work.

But just another specific example that we fixed, Zacharias Mousawi. He didn't fit into the two ways that you could get information. We couldn't prove that he was an agent of a foreign power or that he belonged to a terrorist organization. They don't carry cards anymore. He was acting on his own in concert, ultimately, with another group. So we had to create a third category after the fact, unfortunately.

What it demonstrates is, I think we need to be a little bit more liberal on the front end for the purposes of the protection of the American people, and then make sure that, whether it's minimization procedures or other kinds of protocols that ensure the privacy

of the American people, to put those into place. But looking at the relative challenges and relative threats and relative harms that have occurred so far, it seems that some may be balancing these equities, I think, in the wrong way.

I would hope that as we draw on your expertise—all three of you have been very valuable to this exercise today. As we continue to draw on your expertise, would you also take into account what I am trying to say here? Because as policymakers, we've got to take all of these things into consideration. It seems to me that—well, I've made my point. If any of you would like to comment, I still have a little bit of green left.

Mr. Baker?

Mr. BAKER. Yes, Senator. With respect to the law, I mean, Michael and I both lived through the era of the wall and we can probably go on for quite a bit of time about that.

But let me just say, that's why I focused on creating—urging you to create—a system that's simple and effective. One of the lessons from the wall was, the rules were complex, the rules were misunderstood, and people were afraid of the adverse consequences to their career of making a mistake, so they didn't do what they should have done in certain instances with respect to sharing information.

I think that's one of the things you don't want to have happen here. I think with respect to the current regime that we have, as reflected in the IG's report, you do have confusion about what these statutes allow: you do have confusion with respect to what the scope is, you have confusion about what the standard is.

So, I think that has contributed to the situation that we find ourselves in today. The only other comment I would make is, the IG's report with respect to national security letters are bad facts. I mean, that is a very bad situation. All I would suggest to the Congress, as we all learned in law school, bad cases make bad law. My urging is, don't let that happen.

Senator KYL. But fix the bad cases.

Mr. BAKER. Fix the bad cases, but make sure you don't inadvertently create some other problem.

Mr. NOJEIM. I think if we can learn one thing from the IG reports, it's that people who mean well and are in the business of collecting this information didn't do a good job about following the rules. I think there's just no question about that when you look at the Inspector General reports.

I think there's also no question that some of the reforms that the FBI put in place are going to address some of those problems, but the bigger problems can't be addressed by changing the people who do the work or by changing what work they do. There just has to be a judicial check at some point in this process when the information is particularly sensitive. Again, the principle that we're asking you to abide by is that the more sensitive information ought to be under that judicial check, and that less sensitive identifying information could still be sought without it.

Senator KYL. A final word, Mr. Woods?

Mr. WOODS. All right.

Senator KYL. Again, thank you to all three of you. I appreciate it.

Mr. WOODS. I actually agree with what both of the other witnesses have been saying, in principle. I think the committee should be guided by a rule of proportion. I mean, I read the IG reports and I see errors and ineptitude in the nuts and bolts of this, the kind of right documentation here, what should be uploaded, what shouldn't be uploaded. I do not see, as one sometimes hears in the discussions, a malevolent presence in the government that is bent on subverting people's civil liberties or obtaining information that it should not obtain.

I think the remedy ought to reflect the reality of what's in those reports, which to me means concentrating a lot of effort on that nuts-and-bolts level and not ratcheting up the legal standard that affects every case, or attempting to sort of, you know, throw up our hands and say, this is scary and we're going to try to back off, because that affects the 90 percent of the cases that didn't even have these nuts-and-bolts problems in the IG report. That's what I've been trying to argue, and I'm happy to assist the Committee, as I'm sure my colleagues are.

Senator WHITEHOUSE. Well, I agree with you that there are two very different issues here. One is the very simple, old-fashioned bureaucratic foul-up that took place at the FBI with respect to the implementation process for these NSLs, and that is an important problem. It's a problem that we have drilled into, that the Inspector General has drilled into that I think a variety of initiatives will help to minimize. But every time we touch on this issue I think it raises these larger questions of, really, what the rules are. I don't think we've adapted well enough yet to this modern electronic world in which there are vast pools of information available.

I do think that the privacy of American citizens is a core value in our society and it's a core value for a reason because it affects the balance of power, if you will, between government and citizenry. In a democracy, that is absolutely vital. So I give it, perhaps, a higher value than some of my colleagues do.

But wherever you assign its value, I think I agree with the Senator from Arizona's point, that the American people could feel more comfortable about what information is made available to law enforcement if they had a higher level of comfort with what would happen to it once law enforcement had its hands on it in terms of its duration, maintenance, and all of that, and with what uses it would be put to and who would have access to it.

So I see the question as how you define what the government can get access to, how you define what the government can do with it once it's been allowed to get access to it, and how you define who's allowed to query that pool of information which, in a nutshell, are access, minimization, and predication, as related phenomena that I think this Committee and this Congress are going to have to deal with. I think I will ask you for final comments, because we're nearly done with our time. Your thoughts on how you see those are three related, cross-referencing, interwoven concepts.

Mr. Baker?

Mr. BAKER. Well, I think you're exactly right, Senator. If you look at old FISA that we've been talking about, the original FISA, that required minimization of acquisition in terms of, what does the government get and why; minimization of retention: once

you've gotten it, what do you keep? Do you throw certain things away? Who has access to it? What do they do with it? Where do they store it? How can they look at it? And then minimization of dissemination: Who can they give it to, what purpose can they use it for, and so on.

If you look at the definition of minimization under FISA, I think it's a pretty good one because it says that the Attorney General will approve minimization procedures that will be reviewed by the court and approved by the court, but that—on the one hand, do all that, limit the acquisition, retention, and dissemination of non-relevant, non-pertinent U.S. person information, consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

So you've got to have the right balance, exactly what you're saying. You've got to have the right access to the right data, at the right time, for the right purposes, and to be able to use it effectively for what we all want to accomplish. So I think that is what you are focused on. I think that's exactly right.

I would just add in, as we discussed earlier, you need to think about how long we're going to keep this stuff. As these data bases grow at a certain point in time, what should we be throwing away? Stuff that has not been found to be relevant or pertinent to an investigation in the sense that it's produced a lead that's really, really good during a 5-year period, should we throw it away at that point in time, or what are we going to do with it?

Senator WHITEHOUSE. Mr. Nojeim?

Mr. NOJEIM. It seems to me your ability to control some of the things that you want to control is limited, but is available for some of the things you want to deal with. So, for example, on "what is the quality of the employees that are doing this work, accessing this information?" I don't think you're going to have a lot of control over that.

You'll be able to approve the people at the top, but the people below them you're not going to be able to control that much. "Who in government can get the information once it's uploaded into one of the databases?" I don't think you're going to want to put a lot of limits on that because of the imperative toward information sharing. So you might, but probably won't put limits on that. I think that we're really looking at the front end and the back end.

Senator WHITEHOUSE. Well, the logical limit on that, just to interject, would be not who gets access to it so much as when they get access, the predication question.

Mr. NOJEIM. For what purpose. For what purpose they get access.

Senator WHITEHOUSE. At what point does somebody in the government say, I'm interested in Mr. Nojeim's file, let me pull that up? It shouldn't be just on every government computer. There should be a question that has to be answered first: I need this because X. Particularly in the public corruption world, you've got to predicate before you can go after a public official. I think there's a similar test. It's not just who has access, it's what is required. What's the question that they have, and is it a legitimate question?

Mr. NOJEIM. I think that's exactly right. I think it's very hard to legislate because there are just so many contexts in which you're

going to have to think down the road. I think that it's worth talking about.

I also think, though, where you can be most effective is at the front end and the back end. It's articulating a standard that is what permits the data to get into the data base in the first place, and articulating the minimization procedures that must be followed for getting it cleared out at the end of the day.

Senator WHITEHOUSE. Yes. I appreciate it. Thank you.

Mr. Woods, it looks like you have the final word.

Mr. WOODS. I think that we shouldn't simply take a step because it's easy. It's easy to look at the front end and say we need to change the standard. I really do believe that the core of this is in the sort of middle and back end of this, controlling what is done with information. But I would just end on your point about—

Senator WHITEHOUSE. In terms of the interrelationship, do you agree that if we're going to really get this right we're going to have to focus on not only acquisition, but also minimization and retention and also predication and the querying function, and that those three need to be seen as a coordinated group?

Mr. WOODS. They are all linked. I think—and you're seeing this—as soon as you enter into this question you get pulled into the much broader issue of information sharing, of access to digital information. I think a very important issue, and that is public confidence. Things like the IG report shake public confidence and make the public concerned about these issues. I don't think the public understands how their information is handled, either by the government or by commercial entities. It is a very large question and I think I would just urge the Committee to stick with it. It's not going to be easily resolved, but it desperately needs doing.

Senator WHITEHOUSE. Good.

Well, I want to thank all the witnesses. I think this has been a helpful and interesting day. I would urge you also to stick with it and keep doing your work, and keep hammering on Members of Congress to get to this. We are, I think, in a very interesting time, driven by the technological leaps that we've taken. I will close by repeating the observation I made at the beginning when the Founding Fathers were designing the Fourth Amendment. It never crossed their mind that the sheriff would keep any evidence. It would be thrown out. It would be used at trial and it would be returned, or be destroyed if it was contraband. That was it.

Now we have this facility for maintaining huge amounts of information and it raises a question that, because the Founding Fathers did not face, we can't go and grab an answer off the shelf. This generation has to figure it out based on the principles that have made this country great. I think it's a fascinating topic, and I appreciate your attention to it

The record will remain open for 7 days for any additional submissions anybody chooses to make.

The hearing is hereby adjourned.

[Whereupon, at 11:54 a.m. the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

May 8, 2008

Hon. Patrick Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510-6275

Dear Senator Leahy:

Please find attached my responses to the questions forwarded with your letter of May 1, 2008. These responses are meant to supplement the testimony that I gave on April 23, 2008 during the Committee on the Judiciary hearing regarding "National Security Letters: The Need for Greater Accountability and Oversight."

I would like to thank you, and the other members of the Committee, for inviting me to provide testimony on this complex and highly relevant issue. Having worked with national security letters and similar intelligence authorities while in government, I particularly valued the opportunity to share my perspective with the people who will shape the law in this area. If there is anything I can do to assist you, the other members of the Committee, or your staff as you work with these issues, please do not hesitate to contact me.

Sincerely,

Michael J. Woods

3206 NORTH ROCHESTER STREET • ARLINGTON, VA • 22213
PHONE: 202-725-7589 • E-MAIL: WOODSMICHAELJ@GMAIL.COM

42457.001

Senate Judiciary Committee
Hearing on "National Security Letters:
The Need for Greater Accountability and Oversight"
Wednesday, April 23, 2008

Response of Michael J. Woods to Questions
Submitted by U.S. Senator Russell D. Feingold

1. **In the USA PATRIOT Act, Congress added a new national security letter statute, 15 U.S.C. § 1681v, which permits any government agency involved in counter-terrorism investigations to compel the production of full credit reports. This was in addition to a pre-existing authority, found in 15 U.S.C. § 1681u, which already provided the FBI with NSL authority to obtain some portions of credit reports. But Section 1681u, even as expanded by the Patriot Act, only permitted the FBI to obtain limited information from a credit reporting company with an NSL, and it required a court order for the FBI to obtain a full credit report. You were at the FBI at the time of the Patriot Act. To your knowledge, did the FBI propose or advocate for adding the new Section 1681v?**

Response: To the best of my knowledge, the FBI did not propose or advocate adding the new Section 1681v at the time of the USA PATRIOT Act of 2001. Given the role that I played in preparing the FBI's proposals for the legislation that would become the USA PATRIOT Act, I believe I would have been aware if the FBI had sought the language that became Section 1681v. The FBI proposals that I worked on were all grouped together in Section 505 of the USA PATRIOT Act. The language that established Section 1681v is to be found in Section 358(g) of the Act, among provisions relating to finance and money-laundering.

In fact, I was not aware of the existence of Section 1681v until well after the passage of the USA PATRIOT Act in October of 2001. After the Act was passed, I drafted guidance to all FBI components that summarized the changes made by the USA PATRIOT Act. The document that I drafted describing the new national security letter authorities has been declassified and is appended to my response. As you can see, the document, dated November 28, 2001, describes the changes in the ECPA and RFPA national security letters. However, in describing the revisions to the FCRA national security letter, the document references only Section 1681u (the "FBI only"

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00040 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.002

national security letter). I believe I only became aware of Section 1681v at some point after I left FBIHQ in February 2002.

2. **Government officials, as well as declassified documents issued in response to a FOIA request, have recently confirmed that both the CIA and the Pentagon have issued National Security Letters for financial records.**

   a. **Do you think that agencies other than the FBI should have the authority to issue National Security Letters domestically?**

   b. **What are the disadvantages to allowing multiple agencies, including those whose focus is not on domestic investigations, to issue NSLs?**

Response: I think that the domestic collection of intelligence (regardless of whether it is foreign intelligence or counterintelligence/counter-terrorism information) should occur only under the direct supervision of the Attorney General. I believe that this arrangement offers the best hope of keeping domestic intelligence collection limited and within Constitutional boundaries. This is the manner in which we have regulated domestic intelligence collections since the era of the Church Committee. Executive Order 12,333 mandates that domestic operations, which are primarily conducted by the FBI, conform to guidelines issued by the Attorney General. The Attorney General also approves the Executive Order 12,333 guidelines applicable to other agencies (like the DoD) that have a limited domestic counterintelligence function. Similarly, the Foreign Intelligence Surveillance Act makes the Justice Department responsible for the FISA process and the handling of all requests to the Foreign Intelligence Surveillance Court.

I believe that National Security Letters should be treated in much the same way. Restricting the authority to issue NSLs to the FBI ensures that the letters are issued from an organization that is clearly subject to the Attorney General Guidelines, the DOJ intelligence oversight process, and Congressional reporting requirements. The FBI is unique among U.S. intelligence gathering organizations in that its operational culture is shaped primarily by the criminal law enforcement process. While many see this as inefficiency and argue that domestic collection could be better accomplished by components with a primarily foreign intelligence or military culture, I believe that the criminal law enforcement environment supplies a critical perspective that has contributed to the proper

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00041 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.003

governance of domestic intelligence collection since the late 1970s. That perspective would be lost if the authority to issue NSLs or other forms of compulsory process for domestic collection were distributed outside of the DOJ.

In addition to that broad concern, I see three specific disadvantages to allowing agencies other than the FBI to issue NSLs. First, the production of NSLs outside the FBI increases the likelihood that counterintelligence and counter-terrorism operations will be pursued in an uncoordinated and inefficient manner. At present, those agencies which have limited domestic collection roles (such as the counterintelligence elements of the DoD) have to coordinate their domestic activities with the FBI, which the primary responsibility for domestic counterintelligence and counter-terrorism. The fact that NSLs and other operational authorities are only available through the FBI gives teeth to the policy of coordination, and transforms it into a practical requirement.

Second, the potential for confusion and duplication of effort with respect to the recipients of NSLs increases if the authority is dispersed to other agencies. At present, the FBI is the principal point of contact for the telecommunications providers and financial institutions that are the most common recipients of NSLs. With dispersion of authority to other agencies, these recipients could face multiple requests for the same information and could be confronted with interpretations of the statutory requirements that vary with the agency issuing the NSL. A significant portion of the problems identified by the DOJ Inspector General involved misunderstandings by NSL recipients, and these problems would likely increase if multiple agencies were generating NSLs.

Third, I think the effectiveness of oversight and reporting mechanisms would decline with the dispersion of NSL authority. This is already an issue posed by the present form of Section 1681v, which extends authority broadly to any agency "authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism." The text of the statute does not define "authorized" (as, for example, meaning authorized by Executive Order 12,333) and does not restrict the authority to those agencies that are subject to Attorney General guidelines. There is, to my knowledge, no entity that oversees the implementation of Section 1681v throughout the Executive Branch or collects data on the use of that particular authority. It is difficult to see how real oversight by either the Executive or Congress could occur under these conditions. The 2007 and 2008 Inspector General reports demonstrate how difficult effective oversight is to maintain even within a single agency. I believe that issues such as those noted by the DOJ Inspector General would be likely to multiply were the authority to issue NSLs more broadly distributed.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00042 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.004

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 11/28/2001

To: All Field Offices **Attn:** ADIC;
SAC;
CDC
FCI/IT Supervisors

Counterterrorism AD Watson;
DADs;
Section Chiefs

National Security AD Gallagher;
DADs;
Section Chiefs

From: General Counsel
National Security Law Unit, Room 7975
Contact: [redacted]

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

b7C

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

Case ID #: 66F-HQ-A1255972

Title: NATIONAL SECURITY LETTER MATTERS

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

Reference: 66F-HQ-A1255972 Serial 15

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

11-6-02
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-6-02 BY 60267 NDS/EP/CLT
#966950

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

14) FCRA NSL Checklist

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

1. Introduction to National Security Letters

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

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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00044 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.006

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

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

2. General Policy on the Use of NSL Authority

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

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

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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00045 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.007

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

3. The Mechanics of Producing NSLs

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

A. The NSL

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

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

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

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

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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00046 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.008

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

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

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

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

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

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

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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00047 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.009

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

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

B. The Cover EC

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

1) Field Descriptors

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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00048 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.010

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

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

2) Predication and Relevance

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

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

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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00049 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.011

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

3) Approval

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

4) Reporting Requirements

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

5) Transmittal

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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00050 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.012

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

4. NSL Preparation Assistance

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

Any questions regarding this communication may be directed to [redacted] NSLU, OGC, at [redacted] b7C

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00051 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.013

SUBMISSIONS FOR THE RECORD

Statement of Caroline Fredrickson
Director, Washington Legislative Office

Before
The Senate Judiciary Committee

"National Security Letters:
The Need for Greater Accountability and Oversight"

April 23, 2008

Thank you for the opportunity to submit testimony 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 S. 2088, 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 S. 2088 would provide needed safeguards for civil liberties while preserving government's ability to collect information about individuals who actually pose threats.

We also urge members of the committee to resist the call to expand the FBI's reach into our private lives by creating a blanket subpoena authority. In the face of documented abuse of the four current authorities for discrete categories of records, it is unthinkable that Congress would consider giving the FBI the expanded power over every document and tangible thing. As discussed below, the FBI already has too much access to too much information about too many people. Congress should focus on reining in that authority, not condoning it.

Over the past six years, the ACLU has 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

42457.014

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 have just filed 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, two of which we'd like to address in this statement. 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

---

[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.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00053 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.015

judicial 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.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00054 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.016

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).

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00055 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.017

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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00056 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.018

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. S. 2088 would significantly improve the current statutes by replacing the requirement that the FBI certify "relevance" with a requirement that the FBI certify that the information is actually linked to a suspected agent of a foreign power, his or her associates, or his or her activities. . Specifically, the bill would require proof of specific and articulable facts giving reason to believe that the information or records sought by that letter:

`(i) pertain to a suspected agent of a foreign power; or

`(ii) pertain to an individual who has been in contact with, or otherwise directly linked to, a suspected agent of a foreign power who is the subject of an ongoing, authorized and specifically identified national security investigation (other than a threat assessment); or

`(iii) pertain to the activities of a suspected agent of a foreign power, where those activities are the subject of an ongoing, authorized and specifically identified national security investigation (other than a threat assessment), and obtaining the records is the least intrusive means that could be used to identify persons believed to be involved in such activities.[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

---

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

[25] S. 2088, §§ 2 - 4.

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

[27] 18 U.S.C. § 2709 (2005).

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00057 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.019

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 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]

---

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

[29] 18 U.S.C. § 2709(c).

[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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00058 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.020

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. *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

---

certification must be "treated as conclusive unless the court finds that the recertification was made in bad faith." *Id.*

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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00059 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.021

> 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 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

---

[35] *Id.* at 405.

[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.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00060 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.022

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]

The ACLU believes that S. 2088 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 must include "a statement of specific and articulable facts giving the applicant reason to believe that disclosure of particular information about the existence or contents of a National Security Letter issued under this section will result in—

`(i) endangering the life or physical safety of any person;

`(ii) flight from prosecution;

`(iii) destruction of or tampering with evidence;

`(iv) intimidation of potential witnesses;

`(v) interference with diplomatic relations; or

`(vi) 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]

---

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

[39] S. 2088.§§ 2- 4.

[40] *Id.*

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00061 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.023

The court would be permitted to grant the extension "narrowly tailored to address the specific harm identified by the Government."[41] The bill would permit the FBI to renew the non-disclosure obligation in 180 day increments.

The ACLU believes that S. 2088 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 S. 2088.

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.

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."[42] The blanket letters sought information on 3,860 telephone numbers.[43]

---

[41] *Id.*

[42] 2008 OIG Report at 123.

[43] 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.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00062 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.024

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."[44] 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.[45] 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."[46] 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.[47] 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."[48]

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."[49] 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.[50]

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.[51]

---

[44] *Id.* at 68.

[45] *Id.* at 67.

[46] *Id.* at 68.

[47] *Id.* at 72.

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

[49] 2008 OIG Report at 124.

[50] *Id.* at 127.

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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00063 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.025

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.[52] 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 efforts to rein in the national security letter 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 S. 2088 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.

[52] 2008 OIG Report at 15.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00064 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.026

SECTION BY SECTION OF S. 2088,

THE NATIONAL SECURITY LETTER REFORM ACT OF 2007

NSL = National Security Letter
FBI = Federal Bureau of Investigation
FISA = Foreign Intelligence Surveillance Act
FISC = Foreign Intelligence Surveillance Court
AFP = Agent of a Foreign Power
AG = Attorney General

Sec. 1. Title and Table of Contents. Names the bill "NSL Reform Act of 2007."

Sec. 2. NSLs for Communications Subscriber Records.

Records available: Permits the FBI to obtain subscriber information such as name, address and means of payment on consumers.

- Amends statute so that only "top line" data can be obtained by an NSL. More sensitive information, such as records of actual phone calls made or received, must be obtained through the FISC or grand jury subpoena.

Standard: Records must be relevant to an "ongoing, authorized and specifically identified national security investigation" and that there are specific and articulable facts that the records (i) pertain to a suspected agent of a foreign power, (ii) pertain to an individual in contact with a suspected AFP who is the target of an ongoing authorized and specifically identified investigation, or (iii) pertain to the activities of a suspected AFP who is the target of an ongoing authorized and specifically identified investigation, and obtaining the records "is the least intrusive means that could be used to identify persons believed to be involved in such activities." NSLs should not be issued solely on the basis of First Amendment activity.

- Revokes the overly lenient "relevance" test that has been in place since the PATRIOT Act passed in 2001. The Justice Department's Inspector General (IG) report of 2008 found that just fewer than 50,000 NSLs had been issued in 2006, with a majority of them collecting information on US persons. The 2007 report

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00065 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.027

also found that many NSLs were issued against people two and three times removed from an actual suspected terrorist. It is absolutely vital that Congress rein in this authority by focusing scarce resources on suspects, their associates and their activities instead of trolling through, keeping and using information on innocent individuals.

Gag: Permits the FBI to issue initial 30 day gags with NSLs, if it certifies that the gag is narrowly tailored to meet one of the following harms of disclosure: (I) endangering the life or physical safety of any person; (II) flight from prosecution; (III) destruction of or tampering with evidence; (IV) intimidation of potential witnesses; (V) interference with diplomatic relations; or (VI) otherwise seriously endangering the national security of the US 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. Requires the FBI to affirmatively tell the service provider that the gag is lifted if the facts requiring the gag end before the initial 30 day expiration date.

Allows the government to apply for 180 day extensions of the gag from a federal court on the grounds above.

- The current gag, as amended by the 2006 PATRIOT Reauthorization, authorizes the FBI unilaterally to impose blanket, indefinite, prior restraints on speech and strictly confines an NSL recipient's ability to challenge the gag in court. This past September, a federal court struck down one of the NSL statutes in its entirety after finding the NSL statute's gag provisions violated the First Amendment and the principle of separation of powers. The court held that gag orders must be subject to prompt judicial review and that 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 this kind of judicial review, the statutes are unconstitutional and the government risks losing the NSL authority altogether.

Minimization: Directs the Attorney General to establish minimization procedures governing the retention and dissemination of information collected by NSLs within six months. Procedures shall prohibit nonpublicly available information from being disseminated with identifying information unless it is necessary to understand or assess intelligence information; shall allow for use of information that contains evidence of a crime; and shall provide for return or destruction of information once the person it relates to is no longer of interest or if the information delivered to the FBI is outside the permissible scope of an NSL.

- The Justice Department's Inspector General found that improperly collected information is often uploaded into databases and used by federal agencies. The affirmative requirement to destroy such information set forth in this bill is necessary. Further, the reporting to Congress is far more detailed, and therefore instructive, than the current overall annual number of NSLs that Congress receives. The bill would be even stronger if the use and dissemination of

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00066 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.028

information, especially the destruction of innocent and non-relevant information, was regulated by statute.

Reporting: Requires semiannual reports to the Judiciary and Intelligence Committees about minimization procedures, any court challenges to NSLs, how information gathered by NSLs have helped intelligence investigations and criminal prosecutions.

- The mandatory Congressional reporting is far more detailed, and therefore instructive, than the current overall annual number of NSLs that Congress receives.

Use of Information: Requires the AG to grant authorization before NSL information is used in criminal proceedings. Requires federal, state and local officials to notify a person before NSL information is used against him in a trial, hearing, proceeding, etc. Allows an aggrieved person to seek suppression of NSL information on the grounds that the information was acquired in violation of the Constitution or the NSL statute. If an aggrieved person seeks to suppress NSL information, or discover it in litigation, the government may require the court to review information bearing on that decision in camera by certifying that disclosure would harm national security. Aggrieved persons shall have access to NSL information as governed by the Classified Information Procedures Act.

- Largely tracks with requirements for the use of information collected by trap and trace orders, wiretaps and physical searches under FISA. Requires that access to information by an aggrieved person be governed by the Classified Information Procedures Act that has been in operation for nearly 30 years in the context of criminal, but classified, proceedings.

Sec. 3. NSLs for Financial Records. Permits the FBI to seek the following information from financial institutions: the name and address of the customer; length of relationship with institution; or account numbers.

- Amends statute so that only "top line" data can be received by NSL. More sensitive information, such as actual financial transactions, must be obtained through the FISC or grand jury subpoena.

Applies the standard for issuance, gag, minimization requirements, reporting and use of information as those provisions apply to the communication records NSL discussed above.

Sec. 4. NSLs for Certain Consumer Report Records. Permits the FBI to obtain the following information from a consumer reporting agency: the name and current and former addresses of a consumer; the current and former place of employment of a consumer; and the names and address of financial institutions where the consumer has or had an account.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00067 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.029

Applies the standard for issuance, gag, minimization requirements, reporting and use of information as those provisions apply to the communication records NSL discussed above.

Sec. 5. Judicial Review of NSLs. Allows the recipient of one of the three NSLs above – or of a National Security Act NSL for investigation of US intelligence employees – to challenge a gag before a federal judge on the basis of any legal right or privilege of the recipient, or for the NSLs failure to meet statutory requirements. The court shall review for the standards mentioned above for initial issuance, and determine whether the gag is narrowly tailored. Aggrieved person shall have access to relevant information consistent with the Classified Information Procedures Act.

- The current statutes severely limit the courts' ability to review gags. Indeed, courts are required to treat certain FBI certifications about the need for disclosure as "conclusive" and cannot be set aside unless the certifications are made in bad faith. The Southern District of New York in Doe v. Mukasey found that this violated both the First Amendment and the principle of separation of powers. The constitutionally mandated court review of a prior restraint on speech is whether the gag is narrowly tailored to meet a compelling state interest, and therefore the current statute violates the First Amendment. The court also found that Congress' attempt to thwart the judicial branch's constitutional role violated separation of powers.

Sec. 6. NSL Compliance Program and Tracking Database. Requires tracking of all NSLs, including a copy of the NSL itself, the date of issuance, a description of the information sought, whether it applied to US or non-US persons, the specific authorized investigation it was sought in connection with, whether the information is sought on an actual target of an investigation, when the information was received, and if applicable destroyed, and whether the information was disclosed for law enforcement purposes.

Sec. 7. Public Reporting on NSLs. Breaks down public reporting into the number of NSLs issued for US persons versus non-US persons, and the number of NSLs issued against subjects of investigations and non-subjects.

Sec. 8. Sunset. Returns NSLs to their pre-PATRIOT Act form on December 31, 2009.

- If these statutes were to revert to pre-PATRIOT standards, they would still contain unconstitutional gags. The gag in this bill should not sunset as it provides procedural protections that were absent even in pre-PATRIOT NSLs.

Sec. 9. Privacy Protection for PATRIOT 215 Orders. Require that FISC applications for a court order for "any tangible thing" be based on specific and articulable facts providing reason to believe that they (i) pertain to a suspected AFP, or (ii) a person in contact with an AFP if the circumstances, suggest that the records will be relevant to an ongoing, authorized and specifically identified investigation of that AFP.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00068 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.030

Gags and use of information are governed under the same rules as for NSLs above.

Sec. 10. Judicial Review of 215 Orders. Permits recipients to challenge 215 orders and their attendant gags on the same standards as NSLs above.

- The gag for 215 orders suffers the same failings as the NSL statutes discussed above. Requiring prompt, meaningful review of the gag will prevent First Amendment violations.

Sec. 11. Resources for FISA Applications. Provides additional resources to fund an electronic filing system for FISA applications, personnel and information technology.

- Recent debate has included a number of complaints that the FISA application process is too burdensome. While there is some evidence to the contrary, these new resources will make sure that the FISA process is efficient and responsive to the needs of the government.

Sec. 12. Enhanced Protections for Emergency Disclosures. Amends the Electronic Communications Privacy Act so that companies can voluntarily release records and communications to the government if they have a reasonable belief that there is an immediate danger. The government must notify a court of the disclosure, and the basis for the emergency.

Explicitly authorizes financial institutions and consumer reporting agencies to release records under the same standards and procedures as above.

- The statue currently only requires a "good faith" belief and does not require that the danger be imminent. This returns the statute to pre-PATRIOT levels. The IG found that so-called "exigent" letters were being issued, perhaps in accordance with this section that allows the providers to release information. This would reinvigorate the standard so that extra-NSL sharing of information is truly only in emergency situations, and provides Congress with the information necessary to evaluate whether this provision is being abused. Also creates a new emergency authority to share financial and consumer data with after the fact court notification.

Sec. 13. Data Retention. Clarifies that when the government requests a company to preserve evidence pending a court order or other process, the company wait for the actual order or other process before divulging information.

Sec. 14. Least Intrusive Means. Directs the AG to issue guidelines requiring that the least intrusive means are used in national security investigations. The Guidelines shall include instruction with particular attention to the effect of privacy on individuals, the potential damage to the reputation of individuals and any special First Amendment concerns including NSLs directed libraries or booksellers.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00069 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.031

Statement of James A. Baker
before the
Committee on the Judiciary
United States Senate

April 23, 2008

I. Introduction

Mr. Chairman and Members of the Committee: Thank you for the opportunity to appear here today[1] to discuss National Security Letters (NSLs) and other legal authorities that the government uses to obtain what I will refer to as "non-content information" or "metadata." I define those terms below. In my testimony today, I will endeavor to place the debate about NSLs in the context of the larger legal regime pursuant to which the government collects metadata from a wide variety of sources, and discuss how the government actually uses various legal tools to obtain metadata. In order to understand what changes need to be made to the NSL statutes, it is important to understand how they fit into the larger legal structure that authorizes the collection and use of metadata.

The issues the Committee addresses today are of the utmost importance. As discussed below, the ability of the United States Intelligence Community and law enforcement agencies to collect, retain, and use metadata in an efficient and effective manner that is consistent with American law and values is critical to protecting our liberty and our security in the 21st Century.

I believe that S. 2088, *The National Security Letter Reform Act of 2007*, frames many of the key issues that Congress must address regarding metadata. The bill contains several important improvements to the existing laws governing NSLs and other legal provisions regarding the collection of non-content information. Although the bill makes important changes to the NSL statutes, as discussed below, I believe that additional changes are needed. In particular, in my view Congress should scrap the existing NSL structure and create instead a "national security subpoena" that has the following features: it must be simple and efficient to use; it must be comprehensive in its scope; its use must be subject to robust oversight mechanisms; and its use must be subject to court-approved procedures that require minimization of the acquisition, retention, and dissemination of the metadata that the government obtains, including rules regarding the destruction of collected information after an appropriate time-period. After describing what I mean by non-content information and metadata, I will comment on the existing legal structure and then elaborate on what changes I think are needed.

---

[1] I am appearing here today at the request of the Committee in my personal capacity and the views I express do not necessarily reflect those of my current or former employers. The Department of Justice reviewed this statement and does not object to its publication.

42457.032

II. Metadata

"Metadata" refers to non-content information about communications and activities rather than the actual substance, or "content," of the communications or private activities. Metadata refers to information about a broad array of human activities. It includes information about communications (such as the date, time, and duration of a telephone call), credit card and other financial information, hotel records, airline reservation and frequent flyer records, car rental records, and many other categories of data about our day-to-day activities – where we go, what we buy, and with whom we communicate – and is usually held by third parties such as telecommunications companies, banks, and other private or governmental institutions. As some have said, metadata is information about information, and includes any type of data about an activity that is not itself a substantive communication or a recording of an activity that takes place strictly in private. Metadata would not include the actual words spoken during a telephone call, the subject line or message contained in an email, or a videotape of activities that take place in the privacy of a home. Generally speaking, the Fourth Amendment to the United States Constitution protects the content of communications and other private activities but does not protect non-content information. Even though metadata is not protected by the Fourth Amendment, many people regard it as sensitive and the collection of it as intrusive, which is one of the reasons that Congress has protected certain types of metadata from disclosure through a variety of statutes, such as the Right to Financial Privacy Act (RFPA) and the Electronic Communications Privacy Act (ECPA).

To sum up,m etadata generally is not protected by the Fourth Amendment. But some types of metadata are protected in various ways by federal statutes.

Although we are focusing on the NSL statutes today, there are several other legal provisions that regulate the manner in which the government may obtain and use metadata. These include the Foreign Intelligence Surveillance Act (FISA) pen register and trap and trace statute (50 U.S.C. §§ 1841-1846), the criminal pen register and trap and trace statute (18 U.S.C. §§ 3121-3127), certain provisions of the Electronic Communications Privacy Act (ECPA) (*see, e.g.,* 18 U.S.C. § 2703(d)), and section 215 of the USA PATRIOT Act, as amended (50 U.S.C. §§ 1861-1862). Congress also should review these statutes to determine whether they represent an appropriate balance between liberty and security today. These statutes provide the government with very useful tools for obtaining metadata pursuant to court orders. In some instances, it is highly desirable from both a privacy and security perspective for the government to be required to obtain a court order before collection can begin and for the collection to take place under the supervision of the court; in others, this may represent too cumbersome a process.

At a minimum, Congress should consider amending federal law to require that the government adhere to FISA court-approved minimization procedures with respect to the acquisition, retention, and dissemination of metadata collected pursuant any authority for national security purposes, including NSLs, section 215, the pen register/trap and trace provisions, ECPA, grand jury subpoenas, and voluntary disclosures. Section 215

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00071 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.033

currently requires minimization of the retention and dissemination of collected information, but not the acquisition of such information; similarly, S.2088 only requires minimization of retention and dissemination – not acquisition – of information the government obtains from NSLs only. I address these authorities below as part of the overall scheme under which the government obtains metadata.

III. Overview of the Current Legal Structure

The current legal regime governing the collection and use of metadata is flawed in many respects and must be changed because it places both our security and our liberty at risk. In critiquing and analyzing the current structure and assessing what should be done, it is important to keep in mind the FBI special agents and other intelligence officers who must actually use these tools in fast-paced and potentially high-stakes investigations where it can be very difficult to understand the nature and scope of a threat, or even to know whether a threat actually exists. Metadata can provide investigators with valuable information about the communications, financial, and other links between individuals who make up networks of spies or terrorists; provide investigators with the means to confirm information that they obtain from human sources and informants; and learn basic information about the identity and activities of individuals who are suspected of engaging in unlawful activity. Metadata analysis can represent a less intrusive way of assessing whether individuals are implicated in terrorist or espionage activities, or for determining that they are not involved in such activities and closing investigations of them. The intelligence officials that we charge with protecting our freedom and security are entitled to have available to them metadata collection tools that allow them to do their jobs quickly and effectively without fear of violating the law or the constitutional rights of the people they are sworn to protect. Our current legal structure does not achieve that objective.

The major flaws in the current structure flow mainly from the fact that it is extremely complex, difficult to understand, and hard to implement correctly. This complexity manifests itself in several ways. First, there are often many tools that investigators can use to obtain the same thing. For example, by my count there are at least eight distinct legal tools for collecting telephone call dialing records,[2] such as the numbers involved in a call, and the date, time, and duration of the call. The collection and analysis of such records has been a standard investigative technique for many years for intelligence and criminal investigators in all types of cases, such as investigations of drug dealers, mafia kingpins, white-collar criminals, and terrorists.

The numerous legal tools that are available to investigators differ in important ways. Some of these differences flow from the fact that Congress shaped some of the tools mainly for intelligence investigations, and some were enacted mainly for criminal

[2] These eight methods include: (1) metadata collected as part of a full content FISA order under 50 U.S.C. § 1805; (2) a FISA pen register/trap and trace order under 50 U.S.C. § 1842; (3) a criminal pen register/trap and trace order under 18 U.S.C. § 3123; (4) a FISA business records order (section 215 of the USA PATRIOT Act) under 50 U.S.C. § 1861; (5) a disclosure order under 18 U.S.C. § 2703(d); (6) a National Security Letter (NSL) under 18 U.S.C. § 2709; (7) a federal grand jury subpoena; or (8) voluntary disclosure by an electronic communications service provider under 18 U.S.C. § 2702.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00072 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.034

investigations. In particular, for some tools investigators must demonstrate an adequate connection to an intelligence (or at least national security) investigation and for others they must show a connection to a criminal investigation. Some tools require investigators to go to the Foreign Intelligence Surveillance Court (FISC or FISA court) for authorization while others permit investigators to go to any federal district court. Some require investigators to seek the approval of a federal criminal prosecutor but not a Department of Justice attorney whose responsibilities are intelligence in nature. In reality, however, the FBI now generally treats all national security investigations as just that – national security cases that may have intelligence and/or criminal aspects rather than separate intelligence and criminal investigations.

The tools also differ in the legal standards that investigators must meet. Returning again to telephone dialing records as an example, some tools require investigators to show probable cause,[3] some require relevance to an appropriate investigation, and some require demonstrating specific and articulable facts showing that there are reasonable grounds to believe that the records sought are relevant and material to an ongoing criminal investigation.[4] I discuss these legal standards in somewhat more detail below.

Another significant difference among the tools is their scope. Investigators can use some tools to obtain a wide variety of documents, books, records, or other tangible things (such as grand jury subpoenas and orders under section 215 of the USA PATRIOT Act), while others are much more limited in scope (such as NSLs, which are limited to certain types of communications and financial information). Section 215 is the only metadata tool designed specifically for national security investigators that is comprehensive in scope. Unlike a grand jury subpoena, which only requires the approval of a federal prosecutor, section 215 requires the advance approval of a FISA court judge. Congress should note that this set of circumstances creates incentives for FBI special agents to seek to use grand jury subpoenas whenever possible in order to get around the scope limitations of the NSL provisions and, at the same time, avoid the requirement and added hassle of going to a federal judge.

The tools also differ with respect to the protection they afford to the integrity of the investigation. Some tools permit the government to require the recipient not to disclose the fact that it received an order or a directive, while tools others do not. Such non-disclosure provisions raise several significant legal questions, but, at a minimum, investigators must consider whether such provisions are available when considering whether to implement a particular tool.

---

[3] As noted above, investigators can obtain metadata as part of a full content FISA authorization under 50 U.S.C. § 1805. *See also* 50 U.S.C. § 1801(n) ("'Contents', when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.").

[4] *See, e.g.*, 50 U.S.C. § 1804-1805 (probable cause); 50 U.S.C. § 1861 (relevance); and 18 U.S.C. § 2703(d) (specific and articulable facts).

VerDate Oct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00073 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.035

In addition, the tools differ with respect to nature and scope of the oversight mechanisms in place to ensure compliance with the law. As noted above, some tools require the advance approval of a federal judge and are subject to ongoing monitoring by the court; in other instances FBI officials issue authorizations on their own with no judicial oversight. The government must report on its use of some tools on a regular basis to Congress, while there is no similar reporting requirement with respect to the use of other tools that can be used to obtain the exact same metadata. For example, pursuant to Congressional mandate, the Inspector General of the Department of Justice has conducted extensive oversight of the FBI's use of NSLs and section 215 of the USA PATRIOT Act and issued lengthy reports regarding those matters.[5] In contrast, the FBI regularly uses federal grand jury subpoenas to obtain the exact same type of information available to it through NSLs and 215 orders, and yet the Inspector General has, to my knowledge, not issued any public reports regarding the FBI's use of subpoenas in national security cases even though the implications for the privacy and civil liberties of Americans with respect to the acquisition and use of the metadata are the same.[6]

Another critical difference among the various investigative tools is that some tools require the implementation and use of minimization procedures, or place other restrictions on use of the collected information, while others do not. For example, minimization rules are required for metadata collected pursuant to a section 215 order, but are not required for the same metadata collected pursuant to an NSL. The FBI can also use a grand jury subpoena to obtain the same metadata that it gets from an NSL or a section 215 order, but no minimization procedures are required by statute for information acquired pursuant to a grand jury subpoena, although they may be required by Attorney General guidelines. To be sure, Rule 6 of the Federal Rules of Criminal Procedure limits disclosure of information obtained pursuant to a grand jury subpoena, but such a requirement cannot be said to constitute minimization procedures.

The complexity and variability of the legal tools available to collect and use metadata makes it more likely that investigators will make mistakes that put our security and/or our liberty at risk. For example, it is difficult to effectively train intelligence investigators, agency lawyers, and even smart, energetic law students about the rules for, and risks and benefits of, using the various tools. It also makes it more difficult to conduct proper oversight of the government's acquisition and use of metadata because it can be difficult to determine exactly what authority investigators were relying on to obtain the data. Indeed, because agencies commingle data in databases that they collect from a variety of legal authorities, it is difficult for oversight officials to figure out what is going on and assess whether any violations have occurred. Moreover, as noted above, some tools are subject to extensive external oversight while others are not.

---

[5] *See, e.g.*, Office of the Inspector General, United States Department of Justice, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (March 2008), *available at:* http://www.usdoj.gov/oig/special/s0803b/final.pdf ; and Office of the Inspector General, United States Department of Justice, *A Review of the FBI's Use of Section 215 Orders for Business Records in 2006* (March 2008), *available at:* http://www.justice.gov/oig/special/s0803a/final.pdf.

[6] Of course, grand jury subpoenas do not have the same non-disclosure provisions as the NSL statutes or section 215 of the USA PATRIOT Act that raise First Amendment concerns.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00074 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.036

In addition to posing risks to our liberty, the complexity of the regime also poses significant risks to our security. There is a risk that investigators will hesitate to use a readily available and proper legal tool in novel circumstances, or that they will become enmeshed in extensive legal wrangling and thereby fail to act promptly to prevent an attack or prevent a spy from compromising classified information because they are afraid of making a mistake, violating the law, and getting into trouble.

Thus, the current legal regime for collecting and using metadata is complex to the point of irrationality. It is not consistent with standards of effective management or good government. The American people deserve better.

IV. A National Security Subpoena

In my view, the Intelligence Community needs a single legal mechanism for obtaining authorization to collect, retain and use metadata; it needs a national security subpoena. Investigators should be able to obtain a national security subpoena by meeting one legal standard, which in my view should be relevance to an appropriate national security investigation or to obtain certain types of foreign intelligence information as specified by statute.[7] Only one category of approving official should issue such subpoenas; as I suggest below, that official should be a Department of Justice attorney. National security subpoenas must be comprehensive in scope; they should be available for any type of document, record, or other tangible thing that can be obtained with a federal grand jury subpoena. National security subpoenas must have appropriate non-disclosure provisions that are consistent with the needs of national security and the First Amendment.[8]

A national security subpoena statute should have two other critical features as well – robust oversight mechanisms and a requirement for minimization procedures. Indeed, **Congress should not create a national security subpoena unless it also mandates robust oversight mechanisms for the use of such subpoenas, and requires implementation of court-approved minimization procedures that direct agencies to destroy metadata after an appropriate, but limited, time period – such as five years after the date of collection.** I will address oversight and minimization issues in turn.

Effective oversight of intelligence activities can be difficult. I recently wrote a piece for the *Harvard Journal on Legislation* that discusses some of those challenges.[9] For purposes of my testimony today, suffice it to say that I believe that Congress should require oversight of the use of national security subpoenas in several ways. First,

---

[7] I discuss the relevance standard in greater detail below.

[8] In addition, Congress may want to consider whether to permit agencies other than the FBI to use such national security subpoenas. That is a complex and important question that will require careful evaluation and is beyond the scope of my written testimony today.

[9] *See* James A. Baker, *Symposium Introduction – Intelligence Oversight*, 45 Harvard Journal on Legislation 199 (Winter 2008), *available at*: http://www.law.harvard.edu/students/orgs/jol/vol45_1/baker.pdf.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.037

intelligence investigators should be required to obtain the approval of a Department of Justice attorney – specifically, the Attorney General, the Deputy Attorney General, an Assistant Attorney General, an attorney in the National Security Division of the Department of Justice, or an Assistant United States Attorney[10] – before issuing the subpoena. This is similar to what is required for the issuance of a grand jury subpoena and represents an appropriate balance between the need for meaningful outside review and the need for speed and agility in issuing the large number of subpoenas that are investigators are likely to seek. Agency officials and lawyers do not represent a sufficiently independent oversight mechanism, and the large number of requests for national security subpoenas will overwhelm federal courts. According to the Inspector General of the Department of Justice, the FBI issued more than 49,000 NSLs in 2006 alone. And this number does not include the number of grand jury subpoenas that the FBI requested from federal prosecutors in national security cases.[11]

Congress must also require oversight after the government issues a national security subpoena. The law should mandate that: the Attorney General conduct regular and thorough reviews of the use of national security subpoenas, including assessments of the use of databases and other information technology systems that intelligence agencies use to store and analyze collected information and their compliance with required minimization procedures (discussed below); intelligence agencies make available to the Attorney General all records and information that the Attorney General requires in order to conduct his reviews; Inspectors General conduct periodic audits of the collection, retention, and use of metadata by intelligence agencies; and the Attorney General and the Inspectors General make periodic reports to Congress regarding the results of their reviews.

Congress must also require minimization procedures for the acquisition, retention, and dissemination of information that intelligence agencies obtain through national security subpoenas. As with minimization procedures that Congress now requires for information that agencies collect through full content FISAs, the Attorney General should approve the minimization procedures and the FISA court should review them to ensure that they adequately protect the privacy of Americans consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. The Attorney General and the FISA court should monitor compliance with the minimization procedures. As noted above, the minimization procedures should also mandate destruction of metadata after a reasonable period of time. Although such metadata may retain some foreign intelligence value far into the future, the ability of the metadata to generate actionable foreign intelligence information decreases rapidly and the data should be destroyed after five years from the date of collection in order to limit the privacy impact on innocent Americans.

---

[10] This list intentionally does not include attorneys who are assigned to the FBI or other investigative agencies for the reasons discussed below.

[11] Congress could also consider requiring that national security subpoenas be issued under the authority of the FISA court in order to provide for ongoing court monitoring of the subpoena process similar to what occurs with respect to grand jury subpoenas.

VerDate Oct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.038

If Congress decides not to create a national security subpoena, it should, nevertheless, require that the government implement minimization procedures with respect to the acquisition, retention, and dissemination of metadata that it obtains from whatever source for intelligence purposes. As noted below, the privacy implications of the government's collection and use of vast quantities of personal data are significant. A requirement that the government implement appropriate minimization procedures would go a long way toward enhancing the privacy of all Americans without sacrificing our security. As noted above, S.2088 only includes a requirement that the government minimize the retention and dissemination of NSL information; this should be expanded to include minimization of acquisition so that the government is required to endeavor to limit the amount of information it collects to that which is needed for investigative purposes.

V. The Appropriate Legal Standard

One of the most important things Congress must consider is the legal standard that is appropriate for the FBI or other intelligence agencies to obtain an authorization to collect metadata. As noted above, federal law currently utilizes several standards for obtaining authorization to acquire such information depending upon the legal tool that an investigative agency is deploying. These standards include probable cause, "specific and articulable facts giving reason to believe," and relevance to either a national security or criminal investigation. Prior to the USA PATRIOT Act, the essential standard for an NSL was that the FBI had to have specific and articulable facts giving reason to believe that a particular set of facts existed. My understanding is that this standard has its origins in the criminal law with regard to situations that involve a brief seizure and a relatively non-intrusive search;[12] as noted above, the collection of metadata does not involve a Fourth Amendment search or seizure.[13] The USA PATRIOT Act changed this standard to relevance to an authorized national security investigation. A similar change was made to the FISA business records provision by section 215 of the USA PATRIOT Act and to the FISA pen register and trap and trace statute. Relevance is, and has been, the standard applicable for obtaining criminal pen register and trap and trace authorizations and federal grand jury subpoenas.[14]

While it is understandable that the Committee would want to consider whether to return to the pre-USA PATRIOT Act standard of specific and articulable facts for NSLs following the revelations of abuses of NSL authorities set forth in the 2007 and 2008 Inspector General reports on the FBI's use of NSLs, I urge the Committee to tread

---

[12] *See, e.g., Terry v. Ohio*, 392 U.S. 1, 21 (1967)(". . . in justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion.").

[13] *See* note 2 above.

[14] *See, e.g., United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991) ("[W]e conclude that where . . . a [grand jury] subpoena is challenged on relevancy grounds, the motion to quash must be denied unless the district court determines that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation.").

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00077 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.039

carefully in this area. The Committee could inadvertently render the NSL statutes much less useful as investigative tools and thereby hinder FBI and Intelligence Community investigative efforts to thwart the next attack, or force the FBI to seek federal grand jury subpoenas in whenever possible in national security investigations. As noted above, there is much less oversight of the FBI's use of grand jury subpoenas for national security purposes than there is for other national security investigative tools.

As previously mentioned, I recommend that the appropriate standard for obtaining an NSL or a national security subpoena is relevance to a properly authorized national security investigation or to the collection of specified foreign intelligence information.[15] "Relevance" means having "relation to the matter at hand;"[16] similarly the term "relevant" means "closely connected or appropriate to the matter in hand."[17] By comparison, the Rule 401 of the Federal Rules of Evidence defines "relevant evidence" as, "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."

The standard obviously is broad and the government can use it to justify the collection of a wide range of information. As a result, some are fearful that it will enable the government to conduct wide-ranging "community of interest" investigations or "fishing expeditions" that will result in the collection of vast quantities of information regarding innocent people who are one, two, or three steps removed from the person who is the subject of the investigation. But national security investigations are always about trying to understand the nature of the connections between an individual who officials suspect of posing a threat to the country and others who may be involved in the suspect's threatening activities. The government needs to know whether the connections between a legitimate investigative subject and another person are innocent or nefarious. Metadata collection represents a relatively non-intrusive way of analyzing such connections.

---

[15] Should Congress decide not to create such a subpoena but merely reform the existing NSL statutes, the appropriate standard is still relevance in my view.

[16] *See Merriam-Webster's Online Dictionary*, available at: http://www.merriam-webster.com/dictionary/relevance.

[17] *See Compact Oxford English Dictionary*, available at: http://www.askoxford.com/concise_oed/orexxlevant?view=uk. By comparison, Black's Law Dictionary defines "relevant" as:

> Logically connected and tending to prove or disprove a matter in issue; having appreciable probative value -- that is, rationally tending to persuade people of the probability or possibility of some alleged fact." Cf. MATERIAL (2), (3) "The word 'relevant' means that any two facts to which it is applied are so related to each other that according to the common course of events one either taken by itself or in connection with other facts proves or renders probable the past, present, or future existence or non-existence of the other." James Fitzjames Stephen, A Digest of the Law of Evidence 2 (4th ed. 1881).

Black's Law Dictionary (8th ed. 2004).

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00078 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.040

In assessing whether relevance or some other standard is appropriate for obtaining authorization for metadata collection, it is important to recall how investigations often work. Contrary to traditional counterintelligence investigations or ordinary criminal investigations where you often start with a subject, a victim, or a crime scene, modern national security investigations instead can begin merely with a single piece of information that may or may not signify something of concern.

Take the following example: Assume that the Intelligence Community tells the FBI that a sheet of paper that has a reference to a U.S.-based telephone number was found in a raid at a location overseas where a terrorist operative was living with family members. The only thing written on the paper was the telephone number. There is no indication that the terrorist was actually in contact with that number. The FBI obviously is going to investigate that number as it is relevant to the investigation of the suspected terrorist, even though it may or may not directly "pertain" to him.

The FBI will want to obtain subscriber information about the number, but it will also want to obtain the telephone toll records to see what other numbers the target number has contacted. At this juncture, the FBI may not be able to say that the telephone numbers in contact with the target number pertain to a suspected agent of a foreign power or someone in contact with such an agent. The toll records are, nevertheless, relevant to the investigation because the FBI is trying to see whether the target number has been in contact with any numbers that the FBI or the Intelligence Community has already determined have a terrorist connection. The FBI will also begin to analyze all of the telephone numbers that the target number has contacted that were previously unknown to the FBI. Some of those numbers may be of tremendous investigative interest, such as calls to a nuclear power plant, a U.S. military base, or another sensitive facility. If that is the case, the FBI will then want to look at telephone toll records for the telephone numbers at the sensitive facilities. Again, those numbers are clearly relevant to the investigation, but the FBI may not know whether they pertain to an agent of a foreign power. As you can see, the FBI will now be looking at numbers that are three steps removed from the target number, but that are relevant to an authorized national security investigation. It could go on from there, depending upon what the toll records reveal.

Counterterrorism and counterintelligence investigations are difficult to conduct because the costs of failure are potentially very high, there is always intense pressure to act quickly, and the subjects of the investigation are commingled with the general population and often employ sophisticated tradecraft to conceal their activities and the links between them. Investigators often do not know the identity or location of the subjects or their confederates, and sometimes do not know for sure whether such operatives even exist. Metadata collection and analysis represents an effort to uncover those suspects and the links between them based upon information and knowledge gleaned from other types of investigative activities and analysis. The only workable standard for obtaining metadata in such an environment is relevance to an appropriate national security investigation.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00079 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.041

It is proper to question where the civil liberties protections are in all of this. There are several potential responses to this question. As discussed above, the first way to address concerns about the relevance standard is through robust oversight and a requirement for minimization procedures and data destruction. This is simple to state and easy to include in legislation, but it is difficult, time-consuming, and expensive to do in practice. It is, however, what Congress must do if it wants to ensure that there are adequate protections for the privacy of Americans in a world where the government can and does collect significant quantities of metadata about the activities of innocent Americans. Such procedures would regulate what is acquired and why, who can access the data and for what purpose, who can receive information extracted from the data and what they can do with it, and in what manner and for how long the data can be kept in government files. An appropriate oversight structure requires modern information technology systems to maintain collected data in a secure manner and monitor how it is used.

We also need adequate numbers of competent and independent oversight and compliance officials to make sure that collection authorities are not abused. We need officials whom we can trust to look over the shoulders of the collectors and analysts to ensure that they follow the rules and respect our constitutional rights. Oversight is often an afterthought and viewed as drudgery until there is a revelation of widespread abuse. We need smart people whose integrity is unquestionable consistently watching what is going on.

In addition, Congress could require an NSL or national security subpoena to be relevant to an authorized investigation to obtain certain specified types of foreign intelligence information. David S. Kris suggested this approach in testimony on April 15, 2007, before the Subcommittee on the Constitution, Civil Rights and Civil Liberties of the House Committee on the Judiciary. Mr. Kris's testimony represents a thoughtful approach to many of the issues I have discussed and I commend it to the Committee for its consideration. Mr. Kris's approach would also address a related and difficult question regarding the use of an NSL or a national security subpoena to collect "positive" foreign intelligence, such as information that is relevant to the diplomatic or economic affairs of the United States. I recommend it to the Committee on that point as well.

VI. The Need for Analytical Resources

Notwithstanding what I have said about the importance of metadata to national security investigations, it is important to note that providing effective legal tools for the collection of metadata in a lawful manner is not a panacea. Put differently, just because Big Brother sees more does not necessarily mean that Big Brother knows more. The more information the government collects, the harder it is to sort through this information to find the bad guys. This overlooked fact suggests another area of reform that should be getting at least as much attention from Congress as the scope of the collection authority.

We must ensure that we have enough of the right people in our intelligence agencies to translate, analyze, and act upon all of the intelligence information that we

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00080 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.042

collect. A successful intelligence system has four essential elements: requirements, collection, analysis, and production. We have to seek and collect the right information at the right time – that is, we want timely and accurate intelligence about the right topics – but we also need to process, store, translate, review analyze, produce, and disseminate that intelligence so that military commanders, CIA case officers, and FBI special agents can take prompt action based on it. Poor intelligence is distracting junk, and old intelligence is history.

Advanced information technology systems assist in acquiring, processing, and assessing collected information, but they cannot do the analysis on their own. Only adequate numbers of highly trained and dedicated linguists, analysts, and agents who know their targets well can draw reasonable inferences from the facts, make prudent judgments based on the quality of the intelligence available, and make sound predictions and recommendations to policy-makers.

Moreover, the task is especially hard because, as some have noted, the needle you are looking for is broken into many pieces and most of the pieces are disguised to look like hay. Spies and terrorists don't always identify themselves clearly when they are communicating, they use code words and obscure references to convey meaning, and they rely on a variety of communication modes to transmit messages. More collection will mean more dots available to connect. But intelligence officials will need to do the hard work of connecting them.

VII. Conclusion

Effective and appropriate collection and analysis of metadata is critical to our national security and the protection of our constitutional rights. As I wrote recently in the above-referenced[18] oversight article,

> As the 21st Century progresses, effective oversight of the intelligence community will become even more essential as the risks to our security and our liberty grow. It is likely that the threats we face from hostile foreign powers will only increase over time, as will the government's ability to collect vast amounts of personal information (including our private communications and information about a wide variety of our activities), store that information, and use it in furtherance of its national security objectives. Indeed, at some point in the future any human endeavor that can be represented by digital information will be recorded and stored by someone— either for commercial or public safety reasons—and sooner or later the government will want to acquire some or all of it for foreign intelligence purposes. Telephone toll records, credit card records, and other financial records already provide investigators with powerful tools to track the movements and understand the activities of individuals who are suspected of engaging in improper activities. As more human activity takes place on the Internet, and as technologies improve to enable novel forms of monitoring—for example, the use of face

[18] *See* note 9 above.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00081 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.043

recognition software to track the movement of individuals in public spaces—the volume of data available to intelligence agencies will grow substantially. We will be forced to continually ask: how do we want the government to go about protecting us? And, who will watch our guardians so that they do not become a danger to our freedoms?

The Committee's hearing today is a step forward in addressing these essential questions. In the years to come, we must decide what we mean by terms such as "privacy,"[19] and how much we want the government to know about our activities in exchange for enhancing the government's ability to protect our safety.

I would be happy to address any questions that the Committee may have regarding this matter, and will make myself available to lend any assistance I can with respect to the technical details of draft legislation that the Committee considers now or in the future.

Thank you, Mr. Chairman.

---

[19] *See, e.g.*, "Remarks and Q&A by the Principal Deputy Director of National Intelligence Dr. Donald Kerr, 2007 GEOINT Symposium, Sponsored by the United States Geospatial Intelligence Foundation," October 23, 2007, *available at:* http://www.dni.gov/speeches/20071023_speech.pdf:

> And that leads you directly into the concern for privacy. Too often, privacy has been equated with anonymity; and it's an idea that is deeply rooted in American culture. The Long Ranger wore a mask but Tonto didn't seem to need one even though he did the dirty work for free. You'd think he would probably need one even more. But in our interconnected and wireless world, anonymity – or the appearance of anonymity – is quickly becoming a thing of the past.
>
> Anonymity results from a lack of identifying features. Nowadays, when so much correlated data is collected and available – and I'm just talking about profiles on MySpace, Facebook, YouTube here – the set of identifiable features has grown beyond where most of us can comprehend. We need to move beyond the construct that equates anonymity with privacy and focus more on how we can protect essential privacy in this interconnected environment.
>
> Protecting anonymity isn't a fight that can be won. Anyone that's typed in their name on Google understands that. Instead, privacy, I would offer, is a system of laws, rules, and customs with an infrastructure of Inspectors General, oversight committees, and privacy boards on which our intelligence community commitment is based and measured. And it is that framework that we need to grow and nourish and adjust as our cultures change.
>
> I think people here, at least people close to my age, recognize that those two generations younger than we are have a very different idea of what is essential privacy, what they would wish to protect about their lives and affairs. And so, it's not for us to inflict one size fits all. It's a need to have it be adjustable to the needs of local societies as they evolve in our country.
>
> Eventually, we can only hope that people's perceptions – in Hollywood and elsewhere – will catch up.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00082 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.044

Opening Statement of U.S. Senator Russ Feingold
Senate Judiciary Committee
"National Security Letters: The Need for Greater Accountability and Oversight"

April 23, 2008

The Justice Department's Inspector General documented serious misuse and abuse of National Security Letters from 2003 to 2006. A follow-up audit conducted by the FBI itself not only confirmed the Inspector General's findings, it documented even more violations. These widespread problems are directly attributable to the Patriot Act, which expanded the NSL statutes to essentially grant the FBI a blank check to obtain sensitive information about innocent Americans. Congress gave the FBI very few rules to follow, and it then failed to adequately fix these problems when it reauthorized the Patriot Act.

I appreciate that Director Mueller and others in the FBI leadership ranks have taken these problems seriously. But leaving this to the FBI alone to fix is not the answer.

These Inspector General reports prove that 'trust us' simply doesn't cut it. It was a significant mistake for Congress to grant the government broad powers and just keep its fingers crossed that they wouldn't be misused. Congress has the responsibility to put appropriate limits on government powers – limits that allow agents to actively pursue criminals, terrorists and spies, but that also protect the privacy of innocent Americans.

Congress must also ensure the statute complies with the Constitution. Last fall, a federal district court struck down one of the new NSL statutes, as modified by the Patriot Act reauthorization legislation enacted in 2006, on First Amendment grounds.

That is why I introduced the National Security Letter Reform Act with a bipartisan group of Senators, including Senator Sununu, Senator Durbin, Senator Murkowski, Senator Salazar, Senator Hagel, and others. The bill places new safeguards on the use of National Security Letters and related Patriot Act authorities to protect against abuse and ensure the constitutionality of the statute. Among other things, it restricts the types of records that can be obtained without a court order to those that are the least sensitive and private, and it ensures that the FBI can only use NSLs to obtain information about individuals with some nexus to a suspected terrorist or spy. I am pleased that it has received endorsements from all over the political spectrum, from the Center for American Progress to the League of Women Voters to Grover Norquist of Americans for Tax Reform.

42457.045

United States Senate

WASHINGTON, DC 20510

National Security Reform Act of 2007, S. 2088

November 16, 2007

Dear Colleague,

We urge you to join us in supporting the National Security Letter Reform Act of 2007, S. 2088. This important bipartisan legislation would address problems with the FBI's national security letter (NSL) authorities as highlighted by a March 2007 report by the Inspector General for the Department of Justice. According to that report, the Inspector General found "widespread and serious misuse of the FBI's national security letter authorities. In many instances, the FBI's misuse of national security letters violated NSL statutes, Attorney General Guidelines, or the FBI's own internal policies." In addition, a federal district court recently struck down one of the NSL statutes on First Amendment grounds.

The NSL statutes enable the government in intelligence investigations to obtain three types of personal records – communications records, financial records, and consumer reports – without judicial review. When Congress enacted the USA PATRIOT Act in 2001, it vastly expanded the statutes that authorized the use of NSLs, doing away with the prior requirement that the government have reason to believe that the individual to whom the records pertain is a terrorist or spy. This change meant that the government could use NSLs to obtain the records of individuals three or four times removed from the FBI's suspect, many of whom could be entirely innocent.

This unchecked authority of the executive branch to use NSLs to obtain information about innocent people without judicial review is part of what led to the problems uncovered by the Inspector General's report. The National Security Letter Reform Act corrects these deficiencies in the NSL statutes, and it addresses the constitutional concerns about the secrecy imposed on recipients of NSLs. For example, the bill limits the types of records that can be obtained using NSLs; establishes a standard of individualized suspicion for issuing NSLs; and provides for additional judicial involvement in reviewing the gag orders imposed on recipients of NSLs.

We all agree that going after suspected terrorists needs to be a top priority; this can be done while respecting the privacy of law-abiding Americans. The National Security Letter Reform Act of 2007 is a measured, bipartisan response to a serious problem. It has been endorsed by a range of organizations from a variety of political perspectives. We are pleased that several of our colleagues have already decided to cosponsor the bill, and urge you to join us.

42457.046

November 16, 2007
Page 2

Attached please find a summary of the National Security Letter Reform Act of 2007 and a list of individuals and organizations who have endorsed the legislation. If you would like to cosponsor this bill or have any questions, please let us know, or contact Lara Flint (4-5323) with Senator Feingold's staff or Chip Kennett (4-2841) with Senator Sununu's staff.

Sincerely,

Russell D. Feingold

John Sununu

Richard J. Durbin

Lisa Murkowski

Ken Salazar

Chuck Hagel

THE NATIONAL SECURITY LETTER REFORM ACT OF 2007

The National Security Letter Reform Act of 2007 is a bipartisan response to the Justice Department Inspector General Report detailing the FBI's abuse and misuse of National Security Letters (NSLs). The NSL statutes were vastly expanded by the USA Patriot Act, which essentially granted the FBI a blank check to obtain without judicial approval very sensitive records about Americans, including people not under any suspicion of wrong-doing. The bill addresses the excesses of the Patriot Act that led to the problems uncovered by the Inspector General's report by providing new statutory safeguards and protections – reasonable limitations that retain the FBI's authority to investigate terrorists and spies but also protect the personal information of innocent Americans.

The NSL Reform Act:

- Authorizes the use of National Security Letters to obtain certain less sensitive types of communications records, financial records, and credit report records without judicial review, but with new procedural safeguards to protect against abuse. It no longer permits the use of NSLs to obtain detailed sensitive information about individuals' communications, financial transactions and full credit history.
- Establishes a standard of individualized suspicion for issuing an NSL, requiring that the government have reason to believe the records sought relate to someone with a connection to terrorism or espionage. This replaces the existing relevance standard, which the Inspector General explained could be used to justify obtaining the records of individuals three or four times removed from a suspect, most of whom would be entirely innocent.
- Requires the Attorney General to issue minimization and destruction procedures for information obtained through NSLs, so that information obtained about Americans is subject to enhanced protections and information obtained in error is not retained.
- Places a time limit on the gag order associated with each NSL, which could be extended by the court if the government demonstrates an extension is necessary, and addresses other First Amendment deficiencies identified by a recent federal court decision.
- Requires that the FBI implement a program to ensure compliance with the NSL statutes and establish a tracking database for NSLs.
- Requires more detailed congressional reporting on the use of NSLs.
- Sunsets the NSL statutes on December 31, 2009, when two Patriot Act authorities expire.
- Establishes a standard of individualized suspicion for obtaining a FISA business records order (also known as a "Section 215 order"), and creates procedural protections to prevent abuses.
- Ensures meaningful after-the-fact judicial review procedures for NSLs and Section 215 business records orders and accompanying gag orders.
- Prevents any future use of improper "exigent letters" by strengthening the requirements for using emergency authorities to obtain certain types of business records.
- Directs resources to the FBI and Justice Department for personnel and improved information technology to make the FISA application process more efficient, including an electronic filing system.
- Requires the Attorney General to issue guidelines on using the least intrusive investigative means available in national security investigations, as recommended by the Inspector General.

42457.048

Endorsements for NSL Reform Act

The legislation has the support of individuals and groups including:

- American Booksellers Foundation for Free Expression
- American Civil Liberties Union
- American Conservative Defense Alliance
- American Library Association
- American Policy Center
- Association of American Publishers
- Association of Research Libraries
- The Honorable Bob Barr, Former Member of Congress
- Bill of Rights Defense Committee
- Center for American Progress Action Fund
- Center for Democracy and Technology
- Center for National Security Studies
- Citizen Outreach
- Downsize DC
- Electronic Frontier Foundation
- David Keene, Chairman of the American Conservative Union and Co-Chair of the Constitution Project's Liberty & Security Initiative
- League of Women Voters of the United States
- Liberty Coalition
- Grover Norquist, President of Americans for Tax Reform
- Patriots to Restore Checks and Balances
- PEN American Center
- Republican Liberty Caucus
- Rutherford Institute
- U.S. Bill of Rights Foundation

42457.049

Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee,
Hearing On "National Security Letters:
The Need for Greater Accountability and Oversight"
April 23, 2008

When Congress last reauthorized and expanded the USA PATRIOT Act in March 2006, I voted against it. As I stated then, the Bush administration and the Republican Congress missed an opportunity to get it right. Still, we were able to include some sunshine provisions which have given us insight that we use today in our examination of the use of National Security Letters (NSLs).

I have long been concerned by the scope of the authority for NSLs, and the lack of accountability for their use. Thankfully, we were able to include requirements for a review of the NSL program by the Inspector General in the reauthorization of the PATRIOT Act. For two years now, those reports by the Inspector General have revealed extremely troubling and widespread misuse of NSLs.

The authority to issue NSLs allows the Federal Bureau of Investigation (FBI) to request sensitive personal information – phone bills, email transactions, bank records, and credit reports – without a judge, a grand jury, or even a prosecutor evaluating those requests. In his reports, the Inspector General has uncovered very disturbing misuse of this authority. The Inspector General's reports found widespread violations, including failure to comply with even the minimal authorization requirements and, more disturbingly, that the FBI requested and received information to which it was not entitled under the law. The reports found rampant confusion about the authorities and virtually no checks to ensure compliance or correct mistakes.

Very significantly, the Inspector General also found that NSL use has grown to nearly 50,000 a year and nearly 60 percent of NSLs are used to obtain information about US Persons. This is a major change in the years since 9/11.

I have raised these concerns with FBI Director Mueller and, in fairness, the FBI has acknowledged problems. It has issued new guidance and developed a new data system to track issuance of NSLs. It has also created an Office of Integrity and Compliance to ensure that there are processes and procedures in place to ensure compliance. I believe that the Director and his staff are sincere in their efforts, but I am not persuaded that the actions they have taken are enough.

Today we follow up on earlier oversight hearings to ask what changes are needed to the statutory authority. Among the things that concern me are whether the law should require higher level review and approval – perhaps judicial or Department of Justice review – before NSLs can be issued. Is the standard for issuance, which requires only that it be relevant to a terrorism investigation too lenient? Is the scope of documents available under NSLs too broad? I would also like to hear how we can ensure that there

42457.050

are adequate standards for determining when private records on U.S. persons collected using NSLs can be retained, disseminated, and used.

I commend Senator Feingold, who has been a leader on this issue. I believe his bipartisan bill, the National Security Letter Reform Act of 2007, is on the right track, particularly in its recognition of the need for a real check on and independent oversight of NSLs. The bill would also narrow the extraordinarily broad scope of information that NSLs can acquire and would make the standard for their issuance more rigorous. I look forward to hearing our witnesses' views on this important legislation and getting other ideas from them on possible legislative improvements to NSL authority.

The problem we see with NSLs is just one part of a much broader concern. We all recognize that the changing nature of national security threats, in particular the threat from international terrorism, has required changes to the way the government collects and uses intelligence and the kinds of information it needs. We must remember, though, what a perilous undertaking it is when the government engages in domestic spying. Americans do not like it – with good reason. We have a long history of abuses – the Red Scare of 1919, McCarthyism, COINTELPRO, Watergate, the recent Pentagon Talon database program that collected information on Quakers and other antiwar protesters. If we are going to adapt our collection and use of information from Americans to a changing threat, we must be sure to also do the same for the checks and accountability mechanisms we have to protect the privacy and liberties of Americans.

The FBI's misuse of NSLs is one example of the need for clearly defined procedures and careful controls when collecting and using domestic intelligence, but we must be just as vigilant in other areas. Data mining, use of satellites to collect domestic information, biometrics, fusion centers – these all are tools for national security, but each is fraught with the potential for privacy invasions and harm to Americans' liberties. The Congress has a responsibility to be sure that these domestic intelligence tools are used only with the proper controls and checks to ensure oversight and accountability.

I look forward to hearing from our witnesses this morning.

# # # # #

42457.051

Statement of Gregory T. Nojeim
Director
Project on Freedom, Security & Technology
Center for Democracy & Technology*

before the
Senate Judiciary Committee

National Security Letters
The Need for Greater Accountability and Oversight

April 23, 2008

Chairman Leahy, Ranking Minority Member Specter, and Members of the Committee, thank you for the opportunity to testify this morning.

In reports issued in March 2007 and March 2008, the Inspector General for the Department of Justice found widespread errors and violations in the FBI's use of National Security Letters to obtain bank, credit and communications records of U.S. citizens without judicial approval. These violations are the natural, predictable outcome of the PATRIOT Act and other legal and technology changes, which weakened the rules under which FBI agents issue these demands for sensitive information while dramatically expanding their scope.

In the wake of the Inspector General's first report, the FBI and DOJ promised a series of internal, administrative reforms. In June 2007, the FBI issued detailed guidance on NSLs that contains many useful elements. The latest IG report finds, remarkably, that reforms the IG initially recommended have not been fully implemented. Moreover, the two IG reports taken together demonstrate that the problems posed by NSLs require a legislative solution, not just a bureaucratic one. For example, the IG speculated that lead attorneys in FBI field offices were reluctant to provide an independent review of NSLs for fear of antagonizing the head of the field office. Such reluctance can only be remedied by independent judicial review. No matter how much effort FBI officials make, and despite their undeniable good faith, the only way to truly address the problems that surround NSLs is to reestablish traditional checks and balances, under which a judge must approve governmental access to sensitive information. The National Security Letters Reform Act,

---

* The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the new digital communications media. Among our priorities is preserving the balance between security and freedom after 9/11. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00090 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.092

S. 2088, would put in place standards and procedures for NSLs that would provide much of the necessary oversight.

Let us emphasize at the outset some basic points on which there should be general agreement:

- Terrorism poses a grave threat to our nation. There are people today planning additional terrorist attacks, perhaps involving biological, chemical or nuclear materials.
- The government must have strong investigative authorities to collect information to prevent terrorism. These authorities must include the ability to obtain transactional records or business records of the kind covered by NSLs, data that can help locate a terrorist or uncover terrorist planning.
- Even though current Supreme Court precedent indicates that bank records, communications traffic data, travel records and insurance records are not protected under the Fourth Amendment, they are clearly sensitive and should be protected against unjustified governmental access.
- Therefore, government access to this data must be subject to meaningful controls.

Against this backdrop, we will evaluate here the National Security Letter concept. As we explain below, the current procedures for NSLs, even with the FBI's new internal procedures, are not adequate given the sensitivity of the records at issue. We will offer our recommendations on what should be done.

The Evolution of NSLs: Broad Scope + Low Standards + Secrecy + Indefinite Retention + Widespread Sharing = A Privacy Nightmare

It is helpful first to recall how we arrived at this point. National Security Letters, which started out quite modestly, have grown into something of a monstrosity. Cumulatively, a series of factors have combined to produce a "perfect storm" of intrusive and inadequately controlled power.

The intelligence investigations in which NSLs are issued are not only secretive and long running but also encompass purely legal, even political activity. The PATRIOT Act seriously weakened the standard for issuance of NSLs, loosened internal oversight, and allowed NSLs to be used to get sensitive records on innocent persons suspected of absolutely no involvement in terrorism or espionage. The Intelligence Authorization Act for FY 2004 dramatically expanded the scope of NSLs, so they can now be served on the US Postal Service, insurance companies, travel agents, jewelers, and car dealers, among others. Moreover, agencies other than the FBI have been authorized to issue NSLs, and the number of government officials who can authorize NSLs has been expanded.

In addition, the digital revolution has put in the hands of banks, credit card companies, telephone companies, Internet Service Providers, insurance companies, and travel agents a wealth of information, rich in what it reveals about our daily lives. Information that was

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00091 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.053

previously stored on paper files or incompatible electronic formats is now far easier to transfer, store, manipulate and analyze.

These realities are compounded by the fact that the FBI keeps records for a very long time, even when it concludes that the person to whom the information pertains is innocent of any crime and is not of any continuing intelligence interest. Information is increasingly being shared across agency boundaries, but without audit trails or the ability to reel back erroneous or misleading information, or information that is about people who are of no continuing criminal or intelligence interests. Finally, the PATRIOT reauthorization act made many NSLs for the first time ever compulsory and placed criminal penalties on violation of the non-disclosure requirement (commonly known as a "gag"), changes that probably make it even less likely NSLs will be challenged.

Some of these developments are outside the government's control, driven by changes in technology and business. Some are desirable. Notably, information sharing is needed if we are to connect the dots to prevent terrorist attacks, although legislative and Presidential mandates recognize that information sharing carries threats to privacy. In other regards, the technological and legal changes outlined above may in fact hamper the effectiveness of the government, drowning it in irrelevant information.

Taken together, however, these changes have made National Security Letters a risky power that sits outside the normal privacy rules. Left over from the pre-digital era, they should be replaced with a system of expeditious prior judicial approval when used to seek sensitive personal information.

Undeniably, terrorism poses a serious, continuing threat to our nation. Undeniably, the FBI needs prompt access to some of the kinds of information currently acquired under NSLs. However, given the precipitous legislative weakening of the NSL standards, changes in technology outlined above, and the findings of the IG reports, it is time to conclude that NSLs are in need of a major overhaul.

Self-policing doesn't work. Investigative techniques involving government collection of sensitive information require checks and balances, and those checks and balances must involve all three branches of government. CDT has long recommended adoption of a system of prior judicial approval, based on a factual showing, for access to sensitive information (excluding subscriber identifying information), with a reasonable exception for emergency situations. Going to a judge makes a difference, in a way that is unachievable by merely internal reviews. In an era of cell phones, BlackBerries and ubiquitous Internet access, there is no reason why a system of judicial review and consistent, searching Congressional oversight cannot be designed to serve the government's legitimate needs. In an age where our lives are stored with banks, credit card companies and insurance companies, such a system is vitally needed to protect privacy.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00092 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.054

What Is a National Security Letter?

National Security Letters are simple form documents signed by officials of the FBI and other agencies, with no judicial approval, compelling disclosure of sensitive information held by banks, credit companies, telephone carriers and Internet Service Providers, among others. In total, there are five NSL provisions with compulsory effect:

(1) Section 2709(a) of title 18, United States Code (access to 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 802 of the National Security Act of 1947 (50 U.S.C. 436) (to obtain financial information, records, and consumer reports);
(4) Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) (to obtain certain financial information and consumer reports); and
(5) Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) (to obtain credit agency consumer records for counterterrorism investigations).

In addition, Section 1114(a)(1)(A) – (C) of the Right to Financial Privacy Act (12 U.S.C. 3414(a)(1)(A) – (C)) permits (but does not require) financial institutions, upon request, to disclose financial records to the Department of Defense and any other agency involved in foreign intelligence, counter-intelligence or investigations or analyses related to international terrorism. Finally, 50 U.S.C. Section 436 requires financial institutions and credit bureaus to comply with requests from any authorized investigative agency – including the Department of Defense – for financial information and consumer reports when the records sought pertain to a person who has consented to such access when applying for a security clearance.

Recipients of NSLs are usually gagged from disclosing the fact or nature of a request.

The PATRIOT Act Dramatically Weakened the Standard for NSLs

Before the PATRIOT Act, the FBI and other governmental agencies could issue NSLs only if there was a factual basis for believing that the records pertained to a suspected spy or possible terrorist (in statutory terms, an "agent of a foreign power"). The PATRIOT Act eliminated both prongs of that standard:

- The PATRIOT Act eliminated the requirement that agents provide any factual basis for seeking records. Whatever internal requirements the FBI or another agency may have, there is no statutory requirement that the government articulate the facts showing why it wants the records it seeks.
- The PATRIOT Act eliminated the requirement that the information being sought "pertain to" a foreign power or the agent of a foreign power. Instead, it is sufficient for the FBI to merely assert that the records are "relevant to" an investigation to protect against international terrorism or foreign espionage.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00093 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.055

The PATRIOT Act also expanded FBI issuing authority beyond FBI headquarter officials to include the heads of the FBI field offices (i.e., Special Agents in Charge).

Thus the PATRIOT Act eliminated any effective standard from the NSL authorities. Now, the main requirement is that the FBI must state for internal purposes that the records are "relevant to" or "sought for" foreign counter intelligence or terrorism purposes. Since foreign counterintelligence and terrorism investigations can investigate lawful, even political conduct, and since the FBI conducts wide-ranging investigations on an ongoing basis of many terrorist groups, the requirement that the agents state that the records are sought in connection with some investigation is not a meaningful limit. (Remarkably, the DOJ Inspector General found that FBI agents had issued NSLs without complying even with this minimal administrative requirement.) The requirement that issuance of an NSL for records about a U.S. person not be based solely on First Amendment activities affords very limited protection. It is generally easy for an agent to point to other circumstances that warrant the inquiry.

With these changes, field offices can issue NSLs without providing to anyone outside the Bureau any fact-based explanation as to why the records are sought, and the records sought can be about ***any*** person, even someone not suspected of being a terrorist or spy.

Making Matters Worse: Expanding the Sweep of NSLs

The NSL authority under 12 U.S.C. 3414 allows the FBI to compel disclosure of financial records. A credit card issuer is a financial institution, so an NSL can get the detailed records of where you eat, where you shop, and your other activities. The Intelligence Authorization Act for FY 2004 significantly expanded the reach of this NSL power by expanding the definition of "financial institution" to include a range of businesses that the average person would not consider to be a financial institution:

- travel agencies,
- real estate agents,
- jewelers
- the Postal Service,
- insurance companies,
- casinos, and
- car dealers.

Under the new definition, "financial records" are defined as "any record held by a financial institution pertaining to a customer's relationship with the financial institution." Thus, the new authority permits the use of NSLs for any record held by travel agents, car dealers, or insurance companies, even if the record doesn't relate to financial matters. See Pub. L. 108-177 (Dec. 13, 2004), Sec. 374.[1]

[1] The FBI's June 1, 2007 policy guidance indicates that FBI officials should not use this statutory authority to obtain from such broadly defined "financial institutions'" records that are not "financial in nature."

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00094 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.056

The PATRIOT Reauthorization Act Further Expanded the NSL Power

NSLs were not subject to the original PATRIOT Act "sunsets" and therefore they received little attention in the 2005-2006 debate on reauthorization of the PATRIOT Act. Indeed, the PATRIOT Act reauthorization law[2] actually expanded the NSL power. The reauthorization act gave the government the power to compel record holders to comply with a NSL with a court order and created a new crime, punishable by up to five years in prison, of willful disclosure of an NSL with intent to obstruct an investigation.

The PATRIOT reauthorization act also made it clear that businesses that receive NSLs can challenge them, but this option is not a meaningful protection. Few businesses that receive NSLs have the incentive to challenge them: the cost of providing the records is far less than the cost of hiring a lawyer to challenge the request; the requests are secret, so customers never learn of them and companies cooperating with the government do not have to justify compliance; and the companies that comply have immunity, so even if a customer found out, there would be no statutory remedy against the company that disclosed the records. As we learn from the IG's reports, some companies actually get paid by the government to turn over records pursuant to NSLs.

The PATRIOT reauthorization act clarified that libraries are not subject to NSLs except to the extent they provide email access. The act also required the Inspector General audits that have revealed the problems and further directed the Attorney General and Director of National Intelligence to submit a report on the feasibility of applying minimization procedures to NSLs.

Intelligence Investigations Require More Control, Not Less

Proponents of NSLs frequently argue that they are just like subpoenas in criminal cases, which are issued without prior judicial review. However, intelligence investigations are more dangerous to liberty than criminal investigations – they are broader, they can encompass First Amendment activities, they are more secretive and they are less subject to after-the-fact scrutiny -- and therefore intelligence powers require stronger compensating protections.

First, intelligence investigations are broader. They are not limited by the criminal code. They can investigate legal activity. In the case of foreign nationals in the United States, they can focus solely on First Amendment activities. Even in the case of U.S. persons, they can collect information about First Amendment activities, so long as First Amendment activities are not the sole basis of the investigation.

Secondly, intelligence investigations are conducted in much greater secrecy than criminal cases, even perpetual secrecy. When a person receives a grand jury subpoena or an

---

[2] Pub. L. 109-177 (March 9, 2006), secs. 115-119.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00095 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.057

administrative subpoena in an administrative proceeding, normally he can publicly complain about it. In a criminal case, even the target of the investigation is often notified while the investigation is underway. Most searches in criminal cases are carried out with simultaneous notice to the target. In intelligence cases, in contrast, neither the target nor any of the individuals scrutinized because of their contacts with the target are ever told of the government's collection of information about them. The businesses that are normally the recipients of NSLs are effectively gagged from complaining[3] and are perpetually blocked from notifying their customers that their records have been turned over to the government.

Third, in a criminal investigation almost everything the government does is ultimately exposed to scrutiny (or is locked up under the rule of grand jury secrecy). A prosecutor knows that, at the end of the criminal process, his actions will all come out in public. If he is overreaching, if he went on a fishing expedition, that will all be aired, and he will face public scrutiny and even ridicule. That's a powerful constraint. Similarly, an administrative agency like the SEC or the FTC must ultimately account in public for its actions, its successes and its failures. But most intelligence investigations never result in a trial or other public proceeding. The evidence is used clandestinely. Sometimes the desired result is the mere sense that the government is watching.

Since intelligence investigations are broader, more secretive and subject to less probing after-the-fact scrutiny, protections must be built in at the beginning.

The Digital Revolution Is Eliminating Barriers to Broad Information Gathering and Sharing

The first NSL authorities were granted in 1986, when the Internet was still in its infancy, cell phones were used only by the elites, and banks still mailed canceled checks back to their customers. Today, immensely rich information about our lives is collected by communications service providers, by credit card companies, and in other transactions. Travel agents, insurance companies, and banks all collect computerized information about our actions. Credit cards, cell phones, and the Internet generate digital fingerprints giving a broad picture of our interests and associations.

Not only is the amount of information accessible through NSLs much greater, but the digital revolution has significantly taken the "friction" out of the process of getting information. What used to come in a sheaf (or carton) of paper records now comes on a CD or in an electronic spreadsheet. The government should take advantage of this technology, but there are no longer so many of the practical limits that used to restrain investigators from extending a wide net. Something must substitute for inefficiency.

---

[3] PATRIOT act reauthorization legislation put in place a judicial review process for NSL gags that is nearly meaningless. At the recipient's initiative, a court can set the gag aside only if it finds that there is "no reason to believe" that lifting the gag may endanger national security or have another specified adverse effect, and the government's mere certification that it would have such effect is "conclusive" unless made in bad faith.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00096 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.058

What Do the Inspector General Reports Show?

These facts in combination have turned NLSs into significant threats to personal privacy, and the outlines of that threat can be gleaned from the IG's reports. Some highlights:

- The FBI issued NSLs when it **had not even opened the investigation** that is a predicate for issuing an NSL;
- NSLs are increasingly **used to obtain information about citizens** and lawful permanent residents of the United States. In 2003, only 39% of NSL requests involved records about U.S. persons; this number increased to 57% of NSL requests issued in 2006. This is likely a result of doing away with the requirement that the records sought pertain to an agent of a foreign power because most Americans are not such agents.
- The FBI **retains almost indefinitely the information** it obtains with an NSL, even after it determines that the subject of the NSL is not suspected of any crime and is not of any continuing intelligence interest.
- Data collected with NSLs is made **widely available to law enforcement and intelligence agencies** because it is uploaded into three FBI databases which collectively have tens of thousands of users.
- The return on an FBI NSL often includes information the FBI did not ask for ("**overproduction**") and sometimes includes information which the FBI is barred by statute from obtaining with an NSL.
- **The Attorney General refused to enact minimization procedures** recommended by an NSL Working Group consisting of representatives of the offices of the AG and the DNI. The Working Group, which had acted on a statutory requirement that the AG and DNI study the feasibility of adopting minimization procedures for NSLs, had recommended that NSL data be minimized in conformance with the statutory requirements governing FISA minimization procedures.
- The FBI used **"exigent letters" not authorized by law** to quickly obtain information without ever issuing the NSL that it promised to issue to cover the request.
- The FBI used NSLs to obtain personal information about people **two or three steps removed from the subject** of the investigation.
- The FBI **failed to address the IG's concerns that the lead attorneys in FBI field offices were reluctant to provide an independent review** of NSLs for fear of antagonizing the head of the field office. This is a key finding because the June 1, 2007 FBI guidance puts that in-house review at the center of FBI efforts to ensure that NSL requests are legally sufficient.
- Despite the case-by-case assessment of the need for secrecy required by the PATRIOT reauthorization act, **97% of NSLs gag the recipient,** under pain of criminal penalty, from making disclosures about the NSL it has received.
- In some cases, case agent recitals about the need for non-disclosure were inconsistent with corresponding approval memoranda, showing that these **lead attorneys were not careful in reviewing case agent claims** that the NSL sought had have a gag.
- **The FBI has used NSLs to circumvent adverse rulings of the FISA Court.** After the FISA Court twice refused on First Amendment grounds to authorize an order

VerDate Oct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00097 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.059

under Section 215 of the PATRIOT Act, the FBI issued NSLs to obtain information about the subject based on the same factual predicate it used to seek the Section 215 orders. It did this without first conducting a review to ensure that the investigation did not violate the subject's First Amendment rights.

FBI Guidance Addresses Some of the Problems Identified by the Inspector General

Some of the issues that arise in the context of NSLs can be addressed by administrative changes, but the most important ones cannot. They require a change in the law to establish meaningful judicial oversight.

To begin with, legislation is needed because the problems with NSLs reach beyond the FBI. The FBI issued a June 1, 2007 guidance to put in place procedures to address some of the administrative problems reflected in the 2007 IG report. These new FBI procedures apply only to the FBI, but two of the compulsory NSL statutes – 50 U.S.C. 436, for financial records, financial information and consumer reports, and 15 U.S.C. 1681v, for consumer reports and "all other information in a consumer's file" - permit other governmental agencies to issue NSLs, including the Department of Defense and presumably the CIA. In addition, the DoD and other agencies can issue non-compulsory NSLs under 12 U.S.C. 3414(a)(1).

As the Inspector General report notes, the FBI guidance should reduce the mistakes that FBI agents in the field and FBI attorneys make in issuing NSLs. Thus, the guidance puts in place procedures – and training programs have been conducted -- that will make it less likely that FBI agents seek with NSLs information that they are not entitled to receive. They will make it more likely that agents will not use NSLs to seek information without having first opened the investigation to which the information obtained with the NSL would be relevant. They also make it more likely that when information that was not requested in an NSL is nonetheless provided, the information is returned or destroyed if it is irrelevant, rather than being uploaded to an FBI database and shared with tens of thousands of people. They prohibit the use of "exigent" letters, which are nowhere authorized in the NSL statutes.

However, none of those changes get to the core of the issue, which is to ensure that NSLs are used only in a focused way, when there is a factual basis for believing that the individual whose data is being sought is a terrorist or foreign agent, or the information is otherwise sufficiently important to activities under investigation. The notion that all of the problems with NSLs can be addressed by bureaucratic procedures is fundamentally flawed. It is very hard to control something internally, without the checks and balances normally applied in a democratic system – especially judicial control over demands to seize or compel disclosure of personal information.

Indeed, the FBI guidance leaves the most important questions surrounding NSLs completely unaddressed because these questions are statutory in nature and can be addressed only by Congress. Those questions include:

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00098 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.080

- What kinds of information can be sought with an NSL issued without prior judicial authorization?
- What tie, if any, should there be required to be between the subject of the NSL and a foreign power or the activities of a foreign power?
- What factual showing must be made in order to support an NSL?
- Under what circumstances should the recipient of an NSL be gagged – barred by law from disclosing that an NSL was received and/or complied with?
- What types of objections to a demand for business records are legitimate, and should be heard by a court before compliance with the demand is compelled?
- Which agencies of government should be empowered to issue NSLs?
- Should a different standard apply for NSLs issued for information about a U.S. person than for an NSL issued for information about a non-U.S. person?
- Which NSLs should be mandatory, and which permissive?
- What are the parameters of the minimization procedures that should be adopted to protect information about U.S. persons that is obtained with an NSL?
- What congressional oversight of NSLs is appropriate?

Internal guidance cannot answer these questions. Additional legislation is required. Because the National Security Letter Reform Act provides the right answer to many of these questions, CDT supports the legislation. We also believe that Congress should consider strengthening that legislation by adopting additional reforms.

Reforms Proposed In the National Security Letters Reform Act

CDT has urged Congress to reform NSLs by bringing them under judicial supervision. Under our proposal, access to sensitive personal information would require prior approval of a judge on a showing of specific and articulable facts that the records are relevant to an authorized investigation. The National Security Letters Reform Act, S. 2088 (NSL Reform Act) would creatively advance this goal while preserving the usefulness of NSLs to investigative agencies.

Standards for Access To Less Sensitive Information. First, the bill would separate information that can now be obtained with an NSL into two kinds of information: sensitive personal information and less sensitive personal information. The less sensitive information would continue to be available to the government by means of an NSL, and the standard for issuing the NSL would be tightened. Under S. 2088, the standard for access to less sensitive personal information would be a three part test. There would have to be specific and articulable facts that the information sought pertains to:

> (i) a suspected agent of a foreign power (the pre-PATRIOT Act NSL standard);
> (ii) an individual in contact with, or otherwise directly linked to such a person who is the subject of a national security investigation other than a threat assessment; or
> (iii) the activities of a suspected agent of a foreign power, where those activities are the subject of a national security investigation and obtaining the records is the least intrusive means that could be used to identify persons involved in such activities.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00099 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.061

This NSL standard would permit the government to obtain quickly, and without prior judicial approval, the less sensitive records it needs to protect against terrorism and espionage but it would prohibit the fishing expeditions permitted by current law. The current NSL standard is too loose. Under the current standard, NSLs can be used to obtain information that is merely "relevant" to an investigation to protect against international terrorism, untethered from any suspicion about the individual or any explanation of the connection between the records and the investigation. And, as the IG reports document, the FBI has interpreted the mere relevance standard to permit it to obtain records about people two or three steps removed from the target of the investigation. The June 2007 FBI guidance describes the relevance standard as one that "... is not exceedingly difficult to meet. ... In the context of NSLs, there must be a reasonable belief that the information sought either supports or weakens facts being investigated in a case." This is quite broad.

It is important to note that the FBI guidance indicates that the FBI already prepares paperwork articulating the facts upon which the agent seeking the NSL is relying to support the assertion that the records sought are relevant to the investigation. The articulation is necessary for the internal review that the FBI guidance mandates. Requiring such articulation by statute would not impose a significant additional administrative burden because case agents already prepare a simple factual justification. However, the bill would tie the factual statement to more exacting statutory requirements.

While the proposed standard for issuing NSLs prevents fishing expeditions, it permits use of NSLs to obtain these less sensitive records in circumstances where it is prudent to do so, but would have been impossible under the former agent of a foreign power standard. Suppose, for example, the FBI is trailing a terror suspect and he is seen meeting with another man. The FBI might want to learn more about the second man. But just because someone meets with a suspected terrorist offers no reason to believe that he himself is a terrorist. If the second person were an arms dealer, working only for himself, he would not fit the definition of "agent of a foreign power," but surely the FBI should be able to learn more about him in an intelligence investigation. Under the pre-PATRIOT NSL standard, the FBI could follow the man to learn additional information – arguably a more intrusive technique, and certainly a more costly technique – than using an NSL to obtain the information necessary to determine whether he was of intelligence interest. The NSL Reform Act would permit that NSL to issue; pre-PATRIOT law would not have.

The less sensitive information that could be sought with an NSL is mostly identifying information: name, address, IP address, phone number, means of payment, length of business relationship, account number, name and address of current and past financial institutions and employers, and other relatively less sensitive information.

Standards for Access To More Sensitive Information. Under the NSL Reform Act, information that is more sensitive would still be available to the FBI, but the FBI would have to use other investigative authorities such as orders issued with the approval of a judge under Section 215 of the PATRIOT Act, a subpoena, a judicial order issued under the pen register and trap and trace statutes, or other process permitted by law. Thus,

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00100 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.082

access to more sensitive information in intelligence investigations would require prior judicial authorization. Examples of more sensitive information that would be available under these authorities but not with an NSL include email to/from information, local and long distance toll billing records, and records from financial institutions (broadly defined) other than the less sensitive records mentioned above.

The NSL Reform Act will have the effect of channeling more governmental records requests through the judicial process created under Section 215 of the PATRIOT Act. The NSL Reform Act would also modify Section 215 by permitting the government to obtain records and things only when it has made a showing to a judge that they pertain to a suspected agent of a foreign power or to a person in contact with or otherwise directly linked to such person if the circumstances indicate that the information sought will be relevant to an ongoing national security investigation (other than a threat assessment) of the suspected agent of a foreign power.

The Inspector General reports issued in March 2007 and March 2008 covering Section 215 indicate that reforms are necessary to speed the Section 215 process so that is a viable alternative to using an NSL. The average processing time for a Section 215 order in 2006 was 147 days, and bureaucratic and procedural impediments account for most of that time, according to the reports. It will be necessary for the government to address these delays if Section 215 is to be a useful investigative tool.

Non-Disclosure Requirement: The NSL Reform Act would limit to 30 days the gag that is usually imposed on recipients of NSLs and would tighten the circumstances under which a gag could be imposed. The gag could be extended for additional 180-day periods if the government can prove to a judge that there is reason to believe certain harms specified in the bill would come to pass. The government would bear the burden of proof, and the gag would automatically lapse if the government took no action. This provision is intended to ensure that the gag that can accompany an NSL will pass constitutional muster under the court's reasoning in Doe v. Gonzales, a September 2007 case in which a federal court struck down the gag provision in current law as an unconstitutional prior restraint on speech.

Some tightening of the gag provision is required to make the NSL statutes constitutional, and we support this provision with a modest change. The requirement that the government go to court to extend the gag is problematic because of the enormous burden it would impose on the government. Approximately 50,000 NSLs are issued each year. To require the government to go to court twice a year to extend the gag on most of these NSLs could be an unreasonable burden. In the alternative, we suggest that the NSL recipient be required to initiate the process of lifting the gag, and the government retain the burden of proving the continuing need for the gag. Since most NSL recipients will not seek removal of the gag, this change would ease the burden on the government.

Minimization Procedures. FBI procedures permit it to retain investigative information for 30 years after an intelligence investigation has been closed. Thus, sensitive information obtained with an NSL can be retained for an extensive period. Moreover, there are few

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00101 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.083

limits on the dissemination to other agencies of the information obtained with an NSL. Section 119 of the PATRIOT reathorization act required the Attorney General and the Director of National Intelligence to report to Congress on the feasibility of applying minimization procedures in the context of NSLs to ensure protection of the constitutional rights of U.S. persons. Although an inter-agency NSL Working Group recommended new minimization procedures for NSLs, and the IG made a similar recommendation its 2007 and 2008 reports, adequate minimization procedures have not been adopted.

The NSL Reform Act would correct that deficiency by requiring that minimization procedures be adopted to protect U.S. person information obtained with an NSL. The minimization procedures in the bill are similar to those that govern FISA surveillance, except that those in the bill do not apply to acquisition of information and they require that information about people who are no longer of interest in an investigation be returned or destroyed. Given the mountains of data that are being retained as a result of the growing use of NSLs, and the refusal to date of the responsible agencies to adopt new, adequate minimization procedures, this statutory requirement is necessary.

Additional Reforms

Congress should consider additional reforms that would strengthen the bill. First, it may be advisable to centralize the authority to issue NSLs at the FBI. This would help promote consistent treatment of NSL information and practices across the entire government and would focus congressional and DOJ oversight efforts.

We are particularly concerned that some of the statutes permit the DOD and the CIA both to issue NSLs to seek information about Americans. DOD can issue NSLs for "force protection" purposes – a very broad purpose that has in the past been used to justify domestic spying activities on anti-war activists. It would be consistent with the FBI's role as the governmental entity most responsible for conducting intelligence investigations in the United States for this power to be limited to the FBI. It could also boost much-needed cooperation by encouraging other agencies to work with the FBI instead of conducting uncoordinated parallel investigations. If this reform is adopted, an NSL could issue in most cases only if the FBI had opened an intelligence investigation and the information was sought for that investigation. Other agencies could be permitted to issue NSLs under 50 USC Section 436 only to seek information about government employees with security clearances who have waived their right to privacy with respect to that information.

Recently disclosed documents suggest that the Department of Defense may be referring NSL requests to the FBI and seeking through the FBI access to records it could not obtain issuing its own NSL. We do not see this as necessarily undesirable if the FBI follows proper procedures, and turns down any such requests when statutory requirements and internal guidelines do not permit the FBI to issue an NSL.

Second, Congress should consider requiring disclosure to individuals when their records are obtained by the government in violation of the law. This notification requirement

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00102 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.064

could be limited to cases in which notification would not have a direct adverse effect on national security or any pending investigation.

Finally, it may be appropriate to provide a civil damages remedy to a person aggrieved by a clearly illegal misuse of NSL authorities. The House counterpart to the NSL Reform Act, H.R. 3189, includes a civil damages action "against any person issuing or obtaining the issuing" of such an NSL.

Conclusion

The government has an extraordinarily broad range of powers in intelligence investigations, not only against foreign nationals but also against citizens. Given the secrecy with which these investigations are conducted, their breadth, and the sensitivity of the information that is necessary to conduct a successful investigation, more judicial and congressional oversight need to be built into the process.

The Center for Democracy & Technology is committed to working with this Committee and with the Administration to strike the right balance, to ensure that the government has the tools it needs to prevent terrorism and that those tools are subject to appropriate checks and balances.

I look forward to your questions.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00103 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.085

April 22, 2008

Hon. Patrick J. Leahy, Chairman
Hon. Arlen Specter, Ranking Minority Member
Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

Re: National Security Letters Reform Act, S. 2088

Dear Chairman Leahy and Ranking Member Specter:

The Judiciary Committee will soon consider issues relating to National Security Letters. We write to express our support for the National Security Letters Reform Act (S. 2088).

The PATRIOT Act and Intelligence Authorization Act of FY 2004 drastically expanded the FBI's authority to obtain the business and personal records of Americans by issuing National Security Letters (NSLs). NSLs, which do not require prior judicial approval, can be used to obtain a wide range of documents based upon vague claims that the information is merely "relevant" to a terrorism investigation. Once the FBI acquires records with an NSL, it can keep them indefinitely, even when it concludes that the subject of those records is innocent of any crime and is not of intelligence interest.

Undeniably, the FBI needs prompt access to some of the types of information currently acquired under NSLs, but the current method of self-policing simply does not work. Reports issued by the Office of the Inspector General of the Department of Justice in March 2007 and March 2008 documented the drastic expansion of the use of NSLs and their subsequent abuse. The IG's reports also show that NSLs are increasingly used to obtain records about Americans, making reform all the more important. The NSL Reform Act appropriately addresses the problems uncovered by the Inspector General's reports by establishing statutory safeguards and judicial oversight while protecting privacy concerns and bolstering national security interests.

The bi-partisan NSL Reform Act includes many beneficial reforms. First, it would limit the reach of NSLs by allowing only less sensitive personal information to be made available under this authority. Other existing authorities could still be used to obtain the more sensitive information that would no longer be available with an NSL. It would require the government to determine that records sought with an NSL relate to someone who is connected to terrorism or espionage. The bill would require the Attorney General to issue minimization procedures for information obtained through NSLs, and to create a system to track their use. It would also enhance oversight by requiring additional reporting to Congress. The act would also establish reasonable limits on the "gag" that

42457.086

attaches to an NSL, requiring it to be narrowly tailored and limiting it to 30-days, extendable by a court. The bill would also tighten the standards for court-issued orders under Section 215 of the USA PATRIOT Act (the "library records" provision) by requiring the government to show that the records sought relate to a suspected terrorist or spy, or to someone directly linked to such a person.

We believe this bill takes significant steps toward achieving a balance between privacy and national security concerns. We ask that the Judiciary Committee consider this legislation and report it favorably as soon as is practical. For more information, please contact ACLU's Michelle Richardson, mrichardson@dcaclu.org, 202/715-0825.

Sincerely,
American-Arab Anti-Discrimination Committee
American Civil Liberties Union
American Library Association
American Policy Center
Association of Research Libraries
Bill of Rights Defense Committee
Center for American Progress Action Fund
Center for Democracy & Technology
Constitution Project
Concerned Foreign Service Officers
Defending Dissent Foundation
DownsizeDC.org, Inc.
Electronic Frontier Foundation
Equal Justice Alliance
Federation of American Scientists
Friends Committee on National Legislation
Government Accountability Project
Gun Owners of America
Japanese American Citizens League
League of Women Voters of the United States
Liberty Coalition
The Multiracial Activist
National Security Archive
National Lawyers Guild--National Office
OMB Watch
OpenTheGovernment.org
Unitarian Universalist Service Committee
United Methodist Church, General Board of Church and Society
U.S. Bill of Rights Foundation
cc: Members of the Senate Judiciary Committee

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00105 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.067

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

HEARING ON "NATIONAL SECURITY LETTERS: THE NEED FOR GREATER ACCOUNTABILITY AND OVERSIGHT"

April 16, 2008

Testimony of Michael J. Woods

Mr. Chairman and members of the Committee: I am very pleased to have an opportunity to appear before you this morning. 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 morning 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 direct 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

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00106 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.088

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.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00107 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.089

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.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00108 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.070

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.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00109 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.071

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.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00110 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.072

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 are now appropriate. My understanding is that the goal of change encompasses both addressing the problems identified in the Inspector General Reports and generally enhancing the privacy protections integrated into the statutes. I think that the current crop of legislative proposals offers 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 changing the current statutes.

First, I believe the legal standard for NSLs should remain that of relevance to an authorized investigation and not, as some proposals suggest, 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. Some of the legislative proposals addressing retention provide a good starting point for movement in this direction. A proposal that would further restrict the current ability to disseminate 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.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00111 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.073

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. Language in some of the current proposals certainly represents 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 proposals that would presumptively release security controls after a short period of time as having only the effect of creating a burdensome requirement for court filings in every case. An additional problem with such proposals is that it has a court making what is essentially a classification determination.

Finally, I note that comments here 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 also 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.

VerDate 0ct 09 2002 14:52 May 27, 2008 Jkt 042457 PO 00000 Frm 00112 Fmt 6633 Sfmt 6011 S:\GPO\HEARINGS\42457.TXT SJUD1 PsN: CMORC

42457.074