Testimony of

# Gregory T. Nojeim

April 23, 2008

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, 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 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.

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.

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.

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 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 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 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.

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 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:

? 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.

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, 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 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 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.

* 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.

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."

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

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.