Statement of James X. Dempsey
Policy Director
Center for Democracy & Technology*

before the
House Permanent Select Committee on Intelligence

National Security Letters

March 28, 2007

Chairman Reyes, Ranking Member Hoekstra, and Members of the Committee, thank you for the opportunity to testify this morning.

The Inspector General for the Department of Justice has found widespread errors and violations in the FBI's use of National Security Letters to obtain bank, credit and communications records of US 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 report, the FBI and DOJ have promised a series of internal, administrative reforms. However, the only way to truly address the problem is to change the law and reestablish traditional checks and balances, under which a judge must approve governmental access to sensitive information.

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

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:

- First is the nature of intelligence investigations themselves, which are not only secretive and long running but also encompass purely legal, even political activity.

---

* 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.

- Second was the PATRIOT Act, which 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.
- Third was the Intelligence Authorization Act for FY 2004, which dramatically expanded the scope of NSLs, so they can now be served on the US Postal Service, insurance companies, travel agents, and car dealers, among others.
- Fourth is the digital revolution, which creates 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.
- Fifth is 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.
- Sixth is the imperative to information sharing, so that information is increasingly being shared across agency boundaries, but without audit trails or the ability to reel back erroneous or misleading information.
- Seventh are the changes in the PATRIOT reauthorization act, which made NSLs for the first time ever compulsory and placed criminal penalties on violation of the gag order, 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 judicial approval.

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 report, it is time to conclude that NSLS are outdated and unnecessary.

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 recommends 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 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 reliable

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 (NSLs) are simple form documents signed by FBI officials, 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:

(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).

NSLs are issued in intelligence investigations, which are highly secretive and generally broader than criminal investigations.

The PATRIOT Act Dramatically Weakened the Standard for NSLs

Before the PATRIOT Act, the FBI 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 may have, there is no statutory requirement that the FBI have any reason for wanting 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).

With these changes, field offices can issue NSLs without providing 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.

In one key respect, the Administration was correct in asserting that the pre-PATRIOT standard for NSLS was not workable, namely in its requirement that the information sought had to pertain to a foreign power or an agent of a foreign power. Sometimes the government in a counter-intelligence or international terrorism investigation has a legitimate need for information about a person even though the government has no reason to suspect he is an agent of a foreign power. Suppose, for example, the US government is monitoring the telephone calls of a suspected al Qaeda operative. The government may have no reason to believe that the persons being called by the al Qaeda member are themselves terrorists. But as a first step, the FBI would want to know the names of those persons being called by the al Qaeda, to see if they are otherwise in the FBI's files. Or suppose 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 and find out, for example, where he is employed. 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.

Starting with that legitimate concern, the PATRIOT Act eliminated any effective standard from the NSL authorities. Now, the only 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 issued NSLs without complying even with this minimal administrative requirement.)

Making Matters Worse: Expanding the Sweep of NSLs

The NSL authority under 12 U.S.C. 3414 allows FBI agents 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 by expanding the definition of "financial institution" to include a range of businesses that the average person would not consider to be a bank:

- travel agencies,
- real estate agents,
- 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[1] 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 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 report, some companies actually get paid by the government to turn over records pursuant to NSLs.

The 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 audit that has 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.

After the PATRIOT Act was reauthorized, Sen. Arlen Specter (R-PA) introduced a bill that would have added a much-needed sunset to the NSL provisions, making them expire on December 31, 2009. The Specter bill died in December 2006 at the end of the 109th Congress.

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

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

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 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.

How Can the NSL Authority Be Reformed?

Over the past 2-3 years, the FBI swore that it had NSLs under control. Now the FBI is swearing again that it will adopt further internal procedures to bring NSLs under control. The endeavor 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 for demands to seize or compel disclosure of personal information.

Let us reemphasize 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 that can help locate a terrorist or uncover terrorist planning.
- These investigative authorities must be subject to meaningful controls.
- 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.

CDT is urging Congress to reform NSLs by bringing them under judicial supervision. A starting point would be H.R. 4570, legislation sponsored in the 109th Congress by several members of this Committee. This legislation would --

- require NSLs to be approved by the FISA court or a federal magistrate judge;
- require the government to show a connection between the records sought with an NSL and a terrorist or foreign power;
- create an expedited electronic filing system for NSL applications;
- require the government to destroy information obtained through NSL requests that is no longer needed; and
- mandate more robust congressional oversight, requiring semi-annual reports to both the Congressional Intelligence and Judiciary Committees on all NSLs issued, minimization procedures, any court challenges and an explanation of how NSLs have helped investigations and prosecutions.

These reforms could accommodate an emergency exception, just as FISA and the criminal wiretap law (Title III) have emergency exceptions. It might also be appropriate to continue to authorize FBI officials to get subscriber identifying information (name,

address, data of service) without prior judicial approval. And it will be necessary to work through the limitations of the "agent of a foreign power" standard, in order to address the situations described above, where the government is legitimately interested in a person who it does not have reason to believe agent of a foreign power. The key reform, however, is to require the government, in a few sentences, to state to a judge the factual basis for seeking the records and explain how it expects to use the records to advance its intelligence investigation.

It is important to note that the FBI already prepares much of the paperwork that would be needed to obtain judicial review. It is our understanding that the FBI agents already prepare a factual explanation of their need for the information they are seeking. And we also understand that every NSL already has particularity. These standards should be written into the law, and a judge should be the one to give final approval.

Additional reforms might also be considered, including --

- Requiring disclosure to individuals when their records are obtained by the government in violation of the law and providing a civil remedy for disclosures that are clearly outside the law's standards;
- Expressly limiting the use of "exigent letters;"
- Requiring expungement of information about persons after the government concludes they are unconnected to terrorist activity.

Congress Should Examine Related Issues

We applaud the IG for diligently conducting this Congressionally mandated audit, and we commend the Committee for holding these hearings. However, there are several other issues, of potentially greater magnitude, that should be examined by an appropriate IG and the Congress. One directly related issue is the allegation that the National Security Agency has been conducting real-time interception of call content or communications traffic data inside the US and/or has been obtaining large volumes of transactional data from communications service providers in the United States. The scope of this surveillance could dwarf the NSA program by many magnitudes. Legality aside, it raises many of the same questions as the NSL program: Whether internal controls were in fact followed, whether reporting to Congress was accurate, whether information was being obtained on the wrong persons, etc. Just as it mandated this IG study, Congress should consider mandating an inquiry of the allegations

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 lack of after-the-fact checks and balances, protections of liberty must come up front, in the form of meaningful judicial review based on a factual premise and particularized suspicion.

The Center for Democracy and 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.