Bill Introduced to Reform FBI Data Demands

March 29, 2007

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

The Inspector General for the Department of Justice earlier this month found widespread errors and violations in the FBI's use of "National Security Letters" to obtain bank, credit and communications records of US citizens.

---

(1) FBI Abuse of PATRIOT Powers Entirely Predictable

The Inspector General for the Department of Justice earlier this month found widespread errors and violations in the FBI's use of "National Security Letters" to obtain bank, credit and communications records of US citizens. The key thing to understand about "NSLs" is that they are issued by FBI agents without judicial approval. The violations uncovered by the IG 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. CDT believes that the only way to effectively address the problem is to change the law and apply traditional checks and balances, under which a judge must approve governmental access to sensitive information.

National Security Letters started out as relatively modest exceptions to federal privacy laws, but they 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:

- These data demands are used in intelligence investigations, which can encompass purely legal, even political activity, yet are conducted in secret and without the protections afforded by the criminal justice system.
- The PATRIOT Act seriously weakened the standard for issuance of NSLs 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 of 2004 further 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.
- Meanwhile, there is a steadily growing ocean of data about our daily lives stored in the hands of third parties and available by NSLs: As a result of the digital revolution, banks, credit card companies, telephone companies, Internet Service Providers, insurance companies, and travel agents collect and store a wealth of information about our activities and preferences.
- Once the FBI gets records under an NSL, it keeps them essentially forever, even when it concludes that the subject of those records is innocent.

- Increasingly, the information the FBI collects is being shared with other agencies. In many ways, this is desirable, but it means that misleading information or information about innocent people is being shared across agency boundaries, without audit trails or the ability to reel back erroneous or misleading information.
- The PATRIOT reauthorization act 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.

Taken together, these changes have made National Security Letters a risky power that sits outside the normal privacy rules.

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. NSLs should be replaced with a system of expeditious judicial approval.

Inspector General Report on NSL Abuses [1] (March 2007)

CDT Testimony [2] (March 28, 2007)

House Intelligence Committee Hearing on NSLs [3] (March 28, 2007)

Senate Judiciary Committee Hearing [4] (March 13, 2007)

---

(2) PATRIOT Dramatically Weakened the Standard for FBI Data Demands

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 by removing the requirement that agents provide any factual basis for seeking records and the requirement that the information being sought must "pertain to" a foreign power or the agent of a foreign power. Now 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.

In some respects, the Administration was correct in asserting that the pre-PATRIOT standard for NSLs was not workable, particularly in its requirement that NSLs could be used only to obtain information about 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.

However, the PATRIOT Act went way too far and 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.)

CDT Resources on the PATRIOT Act [5]

---

(3) 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, in some ways 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 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.

---

(4) Bill Introduced to Reform NSL Authority

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. Internal controls are necessary but nowhere near sufficient. NSLs must be subject to the checks and balances normally applied in a democratic system - especially judicial control for demands to seize or compel disclosure of personal information.

Yesterday, Rep. Jane Harman (D-CA) introduced legislation (H.R. 1739) that would require NSLs to be approved by the FISA court or a federal magistrate judge. The bill would also --

- 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 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.

H.R. 1739 [6]

--

Source URL: https://cdt.org/policy/bill-introduced-reform-fbi-data-demands

Links:
[1] http://www.usdoj.gov/oig/special/s0703b/final.pdf
[2] https://cdt.org/testimony/20070328dempsey-nsl.pdf
[3] http://intelligence.house.gov/OpenHearings.aspx?Section=2
[4] http://judiciary.senate.gov/hearing.cfm?id=2616
[5] https://cdt.org/security/010911response.php
[6] http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.1739: