

FRED H. CATE

*Distinguished Professor and Director
Center for Applied Cybersecurity Research
Senior Policy Advisor, Center for Information Policy
Leadership at Hunton & Williams*

Indiana University School of Law—Bloomington
211 South Indiana Avenue
Bloomington, Indiana 47405-7001
Telephone (812) 855-1161
Facsimile (812) 855-0555
E-Mail fcate@indiana.edu

April 14, 2008

The Honorable Jerrold Nadler
Chair, Subcommittee on Constitution, Civil Rights, and Civil Liberties
Committee on the Judiciary
U.S. House of Representatives
B-353 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Nadler:

I regret that prior commitments made it impossible for me to participate in person in your hearing on National Security Letters, but I wish to thank you and your colleagues for holding this hearing and for your foresight in introducing H.R. 3189 (the “National Security Letters Reform Act”). I would also like to offer for the record this brief written statement highlighting the urgent need for the type of discipline and oversight that the National Security Letters Reform Act would impose. This statement reflects my views as a scholar and teacher of information privacy and security law, and should not be attributed to Indiana University nor to any other organization with which I may be affiliated.

National Security Letters

As you well know, four federal statutes authorize the Federal Bureau of Investigation and other agencies to issue “NSLs” to telephone companies, financial institutions, internet service providers, and consumer credit agencies, which require the recipients to produce the records that the government seeks.¹ Following changes made in the USA PATRIOT Act, the government need only state that the records sought are relevant to an authorized international terrorism or counterintelligence investigation and that the investigation is not being conducted “solely on the basis of activities protected by the first amendment” (e.g., not based solely on speech, protect, association, or religious practice). No court is involved, and recipients are prohibited from disclosing the contents or even the existence of an NSL.

While the FBI is required to inform Congress twice a year about its use of NSLs, a report from the Department of Justice Inspector General in 2007 found that the FBI had substantially under-reported to Congress the number of NSL it issued between 2003 and 2005. Instead of the

¹ Right to Financial Privacy Act (1978) (codified as amended at 12 U.S.C. § 3401(a)(5)); the Electronic Communications Privacy Act (1986) (codified as amended at 18 U.S.C. § 2709(b)(2)); the Fair Credit Reporting Act (1970) (codified as amended at 15 U.S.C. § 1681u(a)); the 1994 amendments to the National Security Act (1947) (codified as amended at 50 U.S.C. § 436(A)(1)).

52,199 NSLs reported by the FBI, the actual figure is 143,074.² For 2006, the FBI did not even attempt to report to Congress on its use of NSLs, but instead left that task to the Inspector General, who found that the FBI issued 49,425 NSLs.³

The two Inspector General reports highlight four important features about the FBI's use of NSLs. First, they demonstrate the dramatic growth in the use of NSLs. Not only are many more NSLs issued each year, but each request may seek records concerning many people. In fact, nine NSLs in one investigation sought data on 11,100 separate telephone numbers. The *New York Times* reported in September 2007 that the FBI had issued NSLs seeking data not only about the communications of identified individuals (or telephone numbers), but also of their "community of interest"—the "network of people that the target was in contact with."⁴

Second, the two reports demonstrate the shift in the use of NSLs post-USA PATRIOT Act to increasingly target U.S. persons—from 6,519 in 2003 to 11,517 in 2007.⁵

Third, the Inspector General reports show a pattern of inadequate documentation, inaccurate reporting, poor recordkeeping, inconsistent or erroneous application of internal guidelines, inadequate oversight, incomplete implementation of prior Inspector General requirements, and even inappropriate use of NSLs, resulting in the FBI obtaining information to which it was not legally entitled.⁶

Finally, the Inspector General reports demonstrate plainly the essential need for *external* oversight of the NSL process. It was only because Congress required the Inspector General to report to it on the FBI's use of NSLs—oversight that Justice argued against—that officials within the FBI and Justice, Congress, and the public learned of the FBI's many errors in both its use and reporting of NSLs.⁷ Self-reporting did not work; only investigation by a body external to the FBI disclosed the serious defects in the FBI's use of NSLs and corrected the erroneous information supplied by the FBI to Congress.

The National Security Letters Reform Act

The National Security Letters Reform Act responds to the important lessons of the Inspector General's reports and provides seriously needed tools for ensuring that the NSL power is used appropriately and lawfully. The Act would enhance the oversight provided by courts by giving the recipient of an NSL the right to challenge it and its nondisclosure requirement. It would also give notice to the target of an NSL if the government seeks to use the records

² U.S. Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* 37-38 (2007), available at <http://www.usdoj.gov/oig/special/s0703b/final.pdf>.

³ U.S. Department of Justice, Office of the Inspector General, *A Review of the FBI's Use of National Security Letters* 9 (2008), available at <http://www.usdoj.gov/oig/special/s0803b/final.pdf>.

⁴ Eric Lichtblau, "F.B.I. Data Mining Reached Beyond Initial Targets," *New York Times*, Sept. 9, 2007, at A1.

⁵ 2007 Report, *supra* at 10.

⁶ *Id.* at 10-11.

⁷ USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 119, 120 Stat. 192 (2006).

obtained from the NSL in a subsequent proceeding, and ensure that the target has an opportunity to receive legal counsel and challenge the use of those records.

The proposed law would also strengthen the power of courts to review NSLs by restoring reasonable limits to the purposes for which an NSL may be used. Instead of the vague and expansive “relevant to an authorized investigation” standard, the Act would return to the pre-USA PATRIOT Act requirement that NSLs be based on “specific and articulable facts giving reason to believe that the information or records sought by that letter pertain to a foreign power or agent of a foreign power.” This has the additional benefits of deterring the use of NSLs to target U.S. persons, and building much-needed discipline into the NSL issuing process.

The Act also would give a cause of action to any person aggrieved by the provision of records pertaining to that person as a result of an NSL issued contrary to law or an NSL issued based on a certification made without factual foundation, thus deterring the conduct that the Inspector General found so prevalent at the FBI, and providing an incentive for aggrieved individuals to seek legal protection.

The Act would provide for minimization procedures to ensure that information obtained pursuant to a NSL regarding persons who are no longer of interest in an authorized investigation is destroyed, rather than warehoused in the FBI’s growing Investigative Data Warehouse and other federal databases.

The National Security Letters Reform Act also limits one of the most odious provisions of NSLs—the gag order that the administration in the past has argued could restrict the right of a recipient even to seek legal counsel, much less facilitate accurate recordkeeping and effective political protest. Consistent with other U.S. laws and the First Amendment to the U.S. Constitution, the Act would shift the burden to the government to demonstrate that there is specific cause to justify a prior restraint, shorten the duration of such restraints, and empower courts to review their constitutionality.

Finally, the Act would include a five-year sunset provision, after which the laws governing NSLs would revert to their pre-USA PATRIOT Act form. If the administration believes the broader powers granted by the USA PATRIOT Act in the immediate aftermath of the 9/11 terrorist attacks remain necessary, it would have to make that case to Congress and to the public.

The Broader Context

Before concluding, I would like to briefly address the broader context in which NSLs are used. NSLs are only one example of a wide panoply of tools that the government uses to obtain personal, often sensitive, information about U.S. persons. For example:

- Requests for Wiretap Orders, which allow the government to tap phone lines and do require the authorization of a court, have increased from 1,186 in 1997, to 1,491 in 2001, to 1,839 in 2006. In 2006, on average, each order resulted in 2,685 communications being captured, involving 122 people.

- Requirements for financial institutions and a wide range of other entities to file Currency Transaction Reports and Suspicious Activity Reports have resulted in the government collecting and storing more than 75 million reports over the past decade.⁸
- As of December 2006, the Department of the Treasury had issued 65 administrative subpoenas to the Society for Worldwide International Financial Telecommunication, requiring it to produce as many as all of the 2-3 billion messages about international financial transactions it carries each year.⁹

These are only three examples of the hundreds of ways in which the government collects information about individuals: search warrants, surveillance orders, administrative and law enforcement subpoenas, routine regulatory reporting, new identification requirements, access to other governmental databases (e.g., tax records, vehicle registration, etc.), purchase from a third-party supplier, and the use of fabricated tools such as “exigent letters.” And these don’t include the Terrorist Surveillance Program, Domestic Surveillance Program, the successors to Total Information Awareness, and other classified initiatives through which the government is accessing potentially billions of records about the daily activities and communications of the public. Many of these are not subject to judicial or legislative oversight. And all of the available evidence suggests that government surveillance is growing, and that the data are being retained longer and shared more widely within the government.

In short, NSLs are only one indicator of a sweeping trend in which the government is collecting more and more personal data about its own citizens and mining it for a wide variety of purposes, of which protecting national security is only one. This ubiquitous data collection and use reflects a profound shift in the relationship between the government and the people. The Fourth Amendment to the Constitution reflects the Framers’ hostility to “general searches”—searches not based on specific suspicion. Today, these searches appear increasingly to be the norm, as the government devotes more of its resources to ubiquitous data collection about U.S. persons who have done nothing to warrant suspicion. NSLs are an important place to start, but Congress should be concerned with this broader shift as well.

The National Security Letters Reform Act takes an important step in this direction by limiting the disclosure of information obtained by the government through “exigent letters.” But there is much more to be done to ensure that the government is investing its resources—especially those related to protecting our nation’s security—widely and effectively, and respecting the privacy and constitutionally protected rights of the citizenry.

⁸ Department of the Treasury, *A Report to Congress in Accordance with § 357 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* 4 (2002).

⁹ Belgian Data Protection Commission, Opinion No. 37/2006 of 27 Sept. 2006 on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) Subpoenas, 6. Office of the Privacy Commissioner of Canada, *Commissioner’s Findings* ¶ 30 (Apr. 2, 2007), available at http://www.privcom.gc.ca/cf-dc/2007/swift_rep_070402_e.asp.

What is at Stake

There are compelling reasons for Congress to Act. Protecting privacy is one. As Senator Sam Ervin (D-N.C.) wrote in 1974: “Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets we stand naked before official power.”¹⁰

But in addition to protect privacy, appropriate limits on the indiscriminate storage, collection, and use of personal data by the government are also necessary to enhance our nation’s security. As many people have noted, pursuing data just for the sake of amassing more data, or relying on outdated or unreliable data, is as dangerous to security as to privacy. The intelligence failures that led up to the terrorist attacks have frequently been described as a failure to “connect the dots,” but rarely as a need for more dots. It is hard to believe that the job of “connecting the dots” is made easier by the billions of additional records added to government databases since 2001, and there is growing suspicion that the government’s focus on acquiring more data may be distracting it from the more urgent task of figuring how to make sense of the massive array of data it already has. Moreover, many data-based security tools are of questionable value, since terrorists may be expected to go to great lengths to mask their identities and information, while the government increasingly invests in programs to examine the data of law-abiding citizens.

Effective limits on government access to individual data help to build the discipline into counter-terrorism efforts. By making the government stop and justify its effort to a judge or other senior official, warrant requirements and other privacy protections often help bring focus and precision to law enforcement and national security efforts. In point of fact, courts rarely refuse requests for judicial authorization to conduct surveillance. For example, between 1968 and 2005, courts approved a total of 34,175 wiretap orders (11,861 federal and 22,314 state)—all but 31 sought by the government.¹¹ Between 1979 and 2006, Foreign Intelligence Surveillance Court judges approved 22,984 FISA warrants (40 percent since the September 11, 2001 terrorist attacks)—all but five that the Attorney General had sought.¹² As government officials often note, one reason for these high success rates is the quality of internal decision-making that the requirement to obtain judicial authorization requires. The Inspector General’s reports suggest that in the absence of such a requirement, the FBI’s NSL procedures were sloppy, inconsistent, and failed to ensure compliance with the law.

Appropriate limits on government surveillance also help build public confidence in the government’s national security efforts. Without that confidence, public and political support for promising national security initiatives wanes, and those government employees tasked with the protecting our nation’s security lack the certainty and clear direction necessary to carry out their vital duties. As the Technology and Privacy Advisory Committee appointed to investigate the

¹⁰ Introductory Remarks of Senate Sam J. Ervin on S. 3418, Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579), Senate Committee on Government Operations and House Committee on Government Operations Subcom. on Government Information and Individual Rights, May 1, 1974.

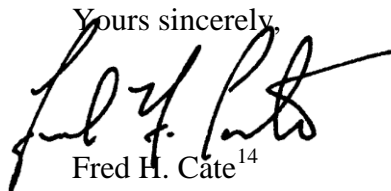
¹¹ Electronic Privacy Information Center, Title III Electronic Surveillance 1968-2005, available at http://www.epic.org/privacy/wiretap/stats/wiretap_stats.html.

¹² Electronic Privacy Information Center, Foreign Intelligence Surveillance Act Orders 1979-2002, available at http://www.epic.org/privacy/wiretap/stats/fisa_stats.html.

Department of Defense's data mining activities noted in the introduction to its recommendations for new privacy protections: "Our conclusion, therefore, that data mining concerning U.S. persons inevitably raises privacy issues, does not in any way suggest that the government should not have the power to engage in data mining, subject to appropriate legal and technological protections. Quite the contrary, we believe that those protections are essential *so that* the government can engage in appropriate data mining when necessary to fight terrorism and defend our nation."¹³

Adopting those appropriate protections is Congress' job. The National Security Letters Reform Act is an important first step. I applaud you for introducing it and for taking it up at tomorrow's hearing. Our nation will be well served if it is adopted into law, and if it is only the first of a series of measures to protect our privacy and enhance our security. Thank you for this opportunity to comment.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Fred H. Cate", written in a cursive style.

Fred H. Cate¹⁴

Distinguished Professor and Director
Center for Applied Cybersecurity Research

¹³ U.S. Department of Defense, Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* 48 (2004),

¹⁴ Fred H. Cate is a Distinguished Professor of Law, Adjunct Professor of Informatics, and director of the Center for Applied Cybersecurity Research at Indiana University, and a senior policy advisor to the Center for Information Policy Leadership at Hunton & Williams. He is a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals; a member of Microsoft's Trustworthy Computing Academic Advisory Board; and reporter for the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information. Professor Cate served as counsel to the Department of Defense Technology and Privacy Advisory Committee, reporter for the third report of the Markle Task Force on National Security in the Information Age, and a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. He is the author of many articles and books, including *Privacy in the Information Age* and *The Internet and the First Amendment*, and *Privacy in Perspective*. He attended Oxford University and received his J.D. and his A.B. with Honors and Distinction from Stanford University. In 2007 *Computerworld* listed him as the only academic on its list of "Best Privacy Advisers" in the United States and Europe.