

**SZADY DECLARATION**

IN THE  
UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF CONNECTICUT

\_\_\_\_\_ )  
 [REDACTED], )  
 AMERICAN CIVIL LIBERTIES UNION; )  
 AMERICAN CIVIL LIBERTIES UNION )  
 FOUNDATION, )  
 )  
 Plaintiffs, )  
 )  
 v. )  
 )  
 ALBERTO GONZALES, in his official capacity )  
 as Attorney General of the United States; )  
 ROBERT MUELLER, in his official capacity as )  
 Director of the Federal Bureau of Investigation; )  
 [REDACTED] in his official capacity as )  
 [REDACTED], Federal Bureau of )  
 Investigation, )  
 )  
 Defendants. )  
 \_\_\_\_\_ )

**FILED UNDER SEAL.**

Civil Action No. 3:05CV1256 JCH

DECLARATION OF DAVID W. SZADY

DAVID W. SZADY, pursuant to 28 U.S.C. § 1746, declares the following under penalty of perjury:

1. I am the Assistant Director of the Counterintelligence Division of the Federal Bureau of Investigation ("FBI"), United States Department of Justice. I have served in this position since March 2002. As part of my official duties, I am responsible for coordinating and supervising various counter-intelligence and counter-terrorism operations of the FBI. I report to the FBI's Executive Assistant Director for Counter-terrorism and Counterintelligence.

2. I have over 30 years of service with the FBI, including 25 years experience in espionage and foreign counterintelligence investigations. During my career, I have served as

Assistant Special Agent in Charge of the FBI's San Francisco Division with responsibility for foreign counterintelligence and terrorism programs, and as chief of the Central Intelligence Agency's ("CIA") Counterintelligence Center's Counterespionage Group.

3. I make this declaration in support of the Government's opposition to plaintiff's motion for a preliminary injunction in connection with the above-captioned action, in which plaintiffs challenge the constitutionality of 18 U.S.C. § 2709. That statute authorizes the FBI to request certain records through what are referred to as "National Security Letters" ("NSLs"), from wire and electronic communication service providers.

**The Nature of Foreign Intelligence and Counter-Terrorism Investigations and the Need for Secrecy in Conducting Such Investigations**

4. As authorized in Executive Order 12333 (entitled "United States Intelligence Activities"), the FBI is the federal agency charged with primary authority to conduct counter-intelligence and counter-terrorism investigations in the United States. See Exec. Order No. 12333 § 1.14(a), 46 Fed. Reg. 59941 (Dec. 4, 1981) ("[T]he Director of the FBI shall . . . [w]ithin the United States conduct counterintelligence and coordinate counterintelligence activities of other agencies within the Intelligence Community.") The Executive Order broadly defines "counterintelligence" to encompass information gathered and activities conducted to protect against, among other things, espionage, other intelligence activities, and international terrorist activities. *Id.* § 3.4(a).<sup>1</sup>

---

<sup>1</sup> Executive Order 12333 is the primary Executive Branch authority for intelligence activities conducted by the United States Intelligence Community. It establishes goals for the collection of intelligence information; assigns responsibilities among the various intelligence components; prescribes what information may be collected, retained and disseminated; and

(continued...)

5. The Executive Order also charges the FBI with conducting counterintelligence activities outside the United States in coordination with the CIA. See *id.* § 1.14(b). The Executive Order further charges the FBI with, within the United States, supporting foreign intelligence collection requirements of other agencies of the Intelligence Community upon request. See *id.* § 1.14(c).

6. The United States government is conducting extensive, world-wide investigations into threats, conspiracies, and attempts to perpetrate terrorist acts and foreign intelligence operations against the United States and its interests abroad. The FBI has been actively conducting its investigations in conjunction with other federal, state and local agencies. Approximately two thousand five hundred FBI agents are engaged in an unprecedented worldwide effort to prevent terrorist attacks by apprehending those responsible for past attacks and by detecting, disrupting, and dismantling terrorist organizations.

7. As the tragic events of September 11, 2001 demonstrated, the catastrophic damage and loss of life that result from terrorist attacks carried out by international terrorist organizations such as al Qaeda present an unparalleled threat to our national security. Terrorists may plan their attacks in secret for years, and then execute their plan with devastating results. The identification and interdiction of those who plan to commit terrorist acts or foreign intelligence operations has become the FBI's most important mission.

8. Counterintelligence and counter-terrorism investigations are different in key respects from traditional criminal investigations. The primary objective of such investigations is

---

(...continued)  
prescribes or proscribes certain techniques that may or may not be used to collect intelligence information.

not to gather evidence for prosecution of past crimes, but rather to disrupt and interdict clandestine intelligence activities and terrorist acts before they occur. Counterintelligence and counter-terrorism investigations are thus forward looking, and often long range. In addition, because foreign intelligence and international terrorist organizations often have many layers and conspirators, one of the goals of counterintelligence and counter-terrorism investigations is to identify as many participants as possible.

9. Accordingly, secrecy in conducting such foreign counterintelligence and counter-terrorism investigations is essential. If targets learn that they are the subjects of investigation, they will likely take action to avoid detection or to disrupt the Government's intelligence gathering. This could include the target's abscondment, destruction of damaging evidence, creation of false evidence, or use of different methods of communication.

10. It is also essential that foreign intelligence and terrorist organizations not learn the scope, focus, or progress of any particular investigation. Armed with such knowledge, these organizations could take action to avoid further detection or to subvert the Government's attempts to thwart any particular planned terrorist act or clandestine intelligence operations. For example, if a terrorist or foreign intelligence organization learns that a particular operative has become the target of an investigation, the organization may substitute that person with a different operative. Similarly, if a terrorist or foreign intelligence organization learns that an investigation has uncovered the proposed location or timing of a planned terrorist attack or clandestine intelligence activity, the organization may alter the location or timing. Terrorist and foreign counterintelligence organizations also benefit from learning what the Government does not yet know, emboldening organizations to act and to accelerate their plans before the Government

identifies them.

11. The need for secrecy continues even after a piece of information has been used against a particular target. If the method or source by which the FBI obtained the information remains secret, the same information can be used in the future against additional targets. By preserving the secrecy of such information, the FBI prevents terrorist groups and foreign intelligence organizations from adjusting their actions to avoid detection and preserves the utility of this information for future investigations. Often, the usefulness of such information against additional targets is not immediately known, and becomes apparent only as additional information is acquired. For this reason, it is important to preserve the secrecy of intelligence acquired in counter-terrorism investigations even where the importance of the information is not immediately apparent -- its usefulness may become apparent only later.

12. As the FBI has determined through its past and ongoing counter-terrorism and counterintelligence investigations, terrorist and foreign intelligence organizations have the sophistication and capability to closely analyze publicly available information concerning the United States' intelligence gathering activities. Terrorist and foreign intelligence organizations can and do piece together publicly available information -- sometimes seemingly innocuous details standing on their own -- to determine the scope, focus, and progress of ongoing counter-terrorism or counterintelligence investigations, and can thereafter use such information to circumvent and disrupt the investigations.

13. Although some general information about how the United States conducts its investigations is publicly available, it is essential that terrorist and foreign counterintelligence organizations not learn exactly how the Government uses its investigative tools in particular

cases. Again, even seemingly innocuous details about the Government's use of a particular investigative tool can be pieced together by terrorist or foreign intelligence organizations to determine patterns and methods of intelligence gathering. Armed with such information, these organizations can tailor their activities to avoid detection in future investigations, and to exploit any perceived weaknesses of our intelligence gathering capabilities.

**The Use of NSLs in Foreign Counterintelligence and Counter-Terrorism Investigations**

14. An NSL issued under 18 U.S.C. § 2709 is one of the tools available to the FBI for conducting its foreign counterintelligence and counter-terrorism investigations.

15. The FBI's past and ongoing counter-terrorism and foreign counterintelligence investigations have revealed that electronic communications play a vital role in advancing terrorist and foreign intelligence activity and operations. Members and agents of international terrorist networks and foreign intelligence organizations use electronic communication services to communicate with each other and to plot future terrorist attacks and clandestine intelligence activities. They also use electronic communication services to build and support their organizations, and to disseminate propaganda.

16. 18 U.S.C. § 2709 authorizes the FBI to request from wire or electronic communication service providers certain records pertaining to their subscribers. Specifically, the statute authorizes the FBI to request subscriber information (including the name, address and length of service of a person or entity receiving services), toll billing records, and electronic communication transactional records pertaining to an account. The statute, however, does not authorize the FBI to obtain the content of any communication, including the subject line, that the

subscriber sends or receives through the provider's services.

17. As a prerequisite to the FBI issuing an NSL pursuant to 18 U.S.C. § 2709, the Director of the FBI or his designee in a position not lower than Deputy Assistant Director at FBI Headquarters or Special Agent in Charge in an FBI field office designated by the Director must certify in writing that the records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. 18 U.S.C. § 2709(b). Further, in accordance with the statute, the certification of the Director or his designee must state that the underlying investigation is not conducted solely on the basis of activities protected by the First Amendment of the Constitution of the United States. *Id.*

**Risks Associated With Disclosure of NSLs**

18. 18 U.S.C. § 2709(c) prohibits any wire or electronic communication service provider (or its agent) from disclosing to any person that the FBI has sought or obtained access to information or records under the statute.

19. The broad non-disclosure provision in § 2709(c) is critical to ensure the integrity and efficacy of foreign counterintelligence and counter-terrorism investigations. Disclosure of the FBI's issuance or use of a particular NSL could compromise counterintelligence and counter-terrorism investigations in a variety of ways.

20. Disclosure of a particular NSL seeking information about a person who is the target of a counter-terrorism or counterintelligence investigation could alert the target that he or she is being investigated by the FBI. The target could then take action to avoid further investigation or to disrupt the ongoing investigation. For example, the target could stop using the

particular communication services related to the NSL, thereby impeding the FBI's ability to monitor his or her activities and to identify other co-conspirators with whom the target is corresponding. The target could also destroy evidence of terrorist or espionage activity, or manufacture false evidence to "throw the FBI off the trail" and impede the investigation. If located in the United States, the target could flee the country before the Government has gathered sufficient evidence to pursue criminal charges, if it elects to do so. The target could also warn other co-conspirators about the FBI's investigation, allowing those co-conspirators to take action to avoid detection or to disrupt intelligence gathering activities. Disclosure of the NSL could also allow the target to discern what specific information the FBI knows about him or her. With such information, the target could tailor any statements he or she makes to the FBI to what he or she believes that the FBI already knows.

21. Disclosure of a particular NSL seeking information about a person who is the target of a counter-terrorism or counterintelligence investigation could also allow terrorist and foreign intelligence organizations to know that a particular operative is under investigation. Armed with that information, these organizations could substitute another operative for the target, warn operatives who are in contact with the target that they may also be the targets of investigation, or use the target to disseminate false information to thwart the FBI's investigation.

22. Even if an NSL seeks information about a person who is not the direct target of an FBI investigation, disclosure of the NSL could allow the person to warn others (particularly those believed to be possible targets of a counter-terrorism or counterintelligence investigation) about the NSL. Such notification could lead the target to discern that the FBI is investigating him or her.

23. Indeed, in criminal investigations, the FBI often is faced with the dilemma of whether to pursue an investigative lead with a third party witness, given the risk that the third party may notify the target of the FBI's investigation. On many occasions, during the covert phase of an investigation, the FBI forgoes pursuing investigative leads with third parties precisely because the risk of notice to the target is too great. The non-disclosure provision in § 2709(c) ensures that, in foreign counterintelligence and counter-terrorism investigations, the FBI is not forced to choose between pursuing relevant information from a third party and risking notification to a target of the investigation.

24. In addition, if an NSL seeks information about a person who is not the direct target of an FBI investigation, maintaining the confidentiality of the NSL serves to protect that person's interests. If that person is found to have no connection to espionage or terrorist activity, non-disclosure of the NSL ensures that the person is not connected -- in the eyes of the public -- to terrorist or counterintelligence activity. Non-disclosure could thus save the person from public harassment and risk of retaliation.

25. Regardless of whether or not a particular NSL seeks information about the direct target of an investigation, disclosure of the particular NSL -- in combination with the disclosure of other NSLs -- could allow terrorist and foreign intelligence organizations to piece together the FBI's individual inquiries and to determine the scope, focus, and progress of particular counter-terrorism or counterintelligence investigations. Terrorist and foreign intelligence organizations could discern that the FBI is investigating particular planned terrorist acts or operations that were discussed through the communication services described in the NSLs, and take action to thwart the investigation of those particular planned acts and operations.

26. Similarly, regardless of whether or not a particular NSL seeks information about the direct target of an investigation, disclosure of any particular NSL - in combination with the disclosure of other NSLs - could allow terrorist or foreign counterintelligence organizations to discern our methods and capabilities of gathering evidence through NSLs. Again, this information can be used to avoid detection in other investigations.

27. Public disclosure of any particular NSL may also adversely impact diplomatic relations with other countries. For example, disclosure of an NSL could reveal the existence of ongoing counterintelligence investigations targeting certain countries. As another example, disclosure of an NSL could jeopardize the confidentiality of an investigation in which other countries may be participating only on the condition that their participation remain confidential.

28. Disclosure of even seemingly non-sensitive information about a particular NSL can jeopardize the integrity of a counter-terrorism or counterintelligence investigation. As stated above, terrorist and foreign intelligence organizations have the capacity to piece together bits of information that, in combination, can (1) reconstruct the scope, focus and progress of a particular investigation, or (2) demonstrate how the FBI gathers intelligence.

29. An important example of seemingly non-sensitive information that might jeopardize a counter-terrorism or counterintelligence investigation is the name of the recipient of an NSL. A disclosure by a particular communication service provider that it has received an NSL may, on its own, seem innocuous, especially if the provider does not name the specific subject of the inquiry or the specific information sought. However, a terrorist or foreign intelligence organization with agents using the service provider in question may thereby learn

which of its communications are potentially compromised, and could instruct its agents not to use, or to give disinformation to, such providers. More broadly, terrorist groups and foreign intelligence can use such information to keep track of how often particular providers receive NSLs, and to avoid providers most likely to receive such inquiries, and thereby to screen their activities from detection.

30. Disclosure of NSLs could also impair the FBI's ability to develop and maintain intelligence sources and assets and cooperating witnesses. The relationship between a source, asset or cooperating witness and the FBI is often based on a promise of confidentiality, including the FBI's assurance that his or her identity will be kept anonymous and that he or she and his or her family will be safe. If a source believed that his or her information would be used as predication in a publicly-available NSL -- particularly if that information were of such a singular nature that its disclosure would identify the source -- the source understandably could be unwilling to cooperate. Similarly, cooperating witnesses would risk being compromised, and their ability to infiltrate and disrupt terrorist and foreign intelligence organizations jeopardized. For example, the nature of the particular information sought in an NSL could permit these organizations to deduce which of their members has decided to cooperate with the authorities, leading not only to a change in tactics by the terrorists or foreign operatives but also to potential reprisals against family members of the suspected cooperator.

#### **Need for Continuing Non-Disclosure of NSLs**

31. Regardless of whether the subject of an NSL remains the target of an ongoing counter-terrorism or counterintelligence investigation, the critical need for non-disclosure of

NSI's continues.

32. As noted above, counterintelligence and counter-terrorism investigations are forward-looking and often long range; unlike criminal investigations, their principal objective is to prevent future clandestine intelligence operations and terrorist attacks. Investigations move from target to target, unearthing the different layers and conspirators of an international terrorist or foreign counterintelligence organization.

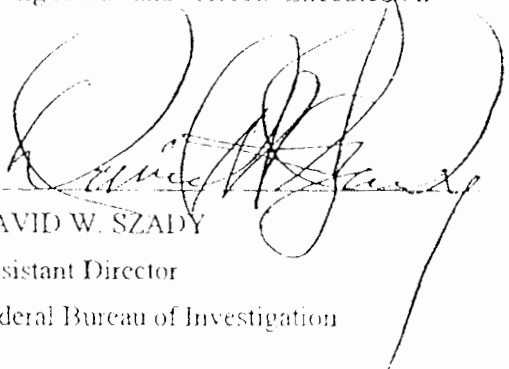
33. Thus, for example, even if the subject of an NSL were arrested and prosecuted, that person may have been in communication with co-conspirators through the services described in the NSL. The FBI's NSL inquiry must remain confidential, to ensure that co-conspirators do not learn that the FBI is aware of the fact that they communicated with the person about whom information was sought through the NSL. This specific example reflects the general principle mentioned above -- that information used against one target may become useful against additional targets in the future, if the source of this information remains unknown. Furthermore, as mentioned above, the future utility of such information often may become apparent only later after additional information is learned. As such there is no natural "end-point" where such information ceases to be useful and the need for secrecy disappears.

34. In addition, an NSL might have been issued based on information provided by a confidential informant; disclosure of the NSL at any time could lead to identification of the confidential informant and retaliation against the informant and/or his family.

35. Moreover, even if the subject of an NSL were arrested and prosecuted, it is critical that remaining terrorist or foreign intelligence operatives not learn how the FBI gathers

intelligence. Data about the particular use of NSIs -- even in completed investigations -- can educate different terrorist and foreign intelligence organizations about how to circumvent and disrupt such intelligence gathering in the future.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 24, 2005, in Washington, D.C.



DAVID W. SZADY  
Assistant Director  
Federal Bureau of Investigation

**EXHIBIT A**



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to  
File No. [REDACTED]

[REDACTED]

[REDACTED]

Dear [REDACTED]

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (as amended, October 26, 2001), you are hereby directed to provide to the Federal Bureau of Investigation (FBI) any and all subscriber information, billing information and access logs of any person or entity related to the following:

[REDACTED]

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.

You are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

You are requested to provide records responsive to this request personally to a representative [REDACTED] of the FBI. [REDACTED] of the records are requested, if available. Any questions you have regarding this request should be directed only to the [REDACTED]. Due to security considerations, you should neither send the records through the mail nor disclose the substance of this request in any telephone conversation or electronic communication.

Your cooperation in this matter is greatly appreciated.

Sincerely,

[REDACTED]

**EXHIBIT B**

URL: <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=18957&c=262>

## **FBI Uses Patriot Act to Demand Information with No Judicial Approval From Organization with Library Records**

August 25, 2005

**NEW YORK –** The American Civil Liberties Union today disclosed that the FBI has used a controversial Patriot Act power to demand records from an organization that possesses “a wide array of sensitive information about library patrons, including information about the reading materials borrowed by library patrons and about Internet usage by library patrons.” The FBI demand was disclosed in a new lawsuit filed in Connecticut, which remains under a heavy FBI gag order.

### **FOR IMMEDIATE RELEASE**

Contact: [media@aclu.org](mailto:media@aclu.org)

### **ACLU Seeks Emergency Court Order to Lift Gag As Congress Prepares to Make Patriot Act Permanent**

**NEW YORK –** The American Civil Liberties Union today disclosed that the FBI has used a controversial Patriot Act power to demand records from an organization that possesses “a wide array of sensitive information about library patrons, including information about the reading materials borrowed by library patrons and about Internet usage by library patrons.” The FBI demand was disclosed in a new lawsuit filed in Connecticut, which remains under a heavy FBI gag order.

The ACLU is seeking an emergency court order to lift the gag so that its client can participate in the public debate about the Patriot Act as Congress prepares to reauthorize or amend it in September.

“Our client wants to tell the American public about the dangers of allowing the FBI to demand library records without court approval,” said ACLU Associate Legal Director Ann Beeson, the lead lawyer in the case. “If our client could speak, he could explain why Congress should adopt additional safeguards that would limit Patriot Act powers.”



Learn more about the  
National Security Letters >>

Papers reveal that the client, whose identity must remain a secret under the gag, "strictly guards the confidentiality and privacy of its library and Internet records." The client is a member of the American Library Association.

The lawsuit challenges the National Security Letter (NSL) provision of the Patriot Act, which authorizes the FBI to demand a range of personal records without court approval, such as the identity of a person who has visited a particular Web site on a library computer, or who has engaged in anonymous speech on the Internet. The Patriot Act dramatically expands the NSL power by permitting the FBI to demand records of people who are not suspected of any wrongdoing.

The lawsuit, *ACLU v. Gonzales*, was filed on August 9, and is pending before Judge Janet Hall of the U.S. District Court in Bridgeport, Connecticut. It names as defendants Attorney General Alberto Gonzales, FBI Director Robert Mueller, and an FBI official whose identity remains under seal. Both the national ACLU and its Connecticut branch said they were forced to file the lawsuit initially under seal to avoid penalties for violating the gag provision, which they are challenging on First Amendment grounds.

The court has set an emergency hearing for Wednesday, August 31, 2005 on the ACLU's request to lift the gag.

Whether the Patriot Act has been used to obtain information about library patrons has been a flashpoint in the Patriot Act debate. The government has repeatedly dismissed the concerns of librarians that the act could force them to violate their ethical responsibility to protect the privacy of library users. Former Attorney General John Ashcroft even called these concerns about the Patriot Act "baseless hysteria."

Congress is currently undertaking efforts to reauthorize the Patriot Act, with both the House and Senate having passed different versions of legislation before adjourning for the August recess. While the ACLU has not endorsed either bill, it has said the Senate bill takes steps in the right direction.

"As Congress comes back to work out the differences in the House and Senate bills to reauthorize the Patriot Act, a commitment to freedom must prevail," said Caroline Fredrickson, Director of the ACLU Washington Legislative Office. "The more we learn about the Patriot Act, the clearer it is that too much power was granted to the government, with too few safeguards against abuse. While neither reauthorization bill is perfect, we call on Congress to use the Senate bill as its guide as it reconsiders the Patriot Act."

In an earlier ACLU lawsuit challenging the NSL power, a federal court issued a landmark decision in September 2004 striking down the NSL statute, saying that

"democracy abhors undue secrecy." The court held that the NSL law violates the First and Fourth Amendments, but allowed the law to stand while the government is appealing the decision.

The United States Court of Appeals for the Second Circuit is expected to hear the government's appeal of that lawsuit this fall. The government recently asked the court to delay the appeal while Congress debates reauthorization of the Patriot Act. However, the ACLU opposes any delay, citing the need for urgent court action so that its John Doe client in the first lawsuit can also participate in the public debate.

"Judicial review is a key part to our system of checks and balances," said Anthony D. Romero, Executive Director of the ACLU. "As we consider expanding and extending the Patriot Act, this case shows us what might become routine if we don't fix the law."

The ACLU has created a special Web page on its National Security Letter litigation, which includes links to today's legal papers, online at [www.aclu.org/nsll](http://www.aclu.org/nsll).

Attorneys in the case are Beeson, Jameel Jaffer and Melissa Goodman of the national ACLU and Annette M. Lamoreaux of the ACLU of Connecticut.

The redacted version of the ACLU's complaint is available online at: <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=18956&c=262>.

© ACLU, 125 Broad Street, 18th Floor New York, NY 10004 This is the  
of the American Civil Liberties Union and the ACLU Foundation  
Learn more about the distinction between these two components of the

[User Agreement](#) | [Privacy Statement](#) | [FAQs](#)

**EXHIBIT C**

washingtonpost.com

## Library Challenges FBI Request

Patriot Act Prohibits Details of Lawsuit From Being Released

By Dan Eggen  
Washington Post Staff Writer  
Friday, August 26, 2005; A11

A member of the American Library Association has sued the Justice Department to challenge an FBI demand for records, but the USA Patriot Act prohibits the plaintiff from publicly disclosing its identity or other details of the dispute, according to court documents released yesterday.

The lawsuit comes as Congress prepares to enter final talks over renewal of the Patriot Act, a counterterrorism law that was overwhelmingly approved after Sept. 11, 2001. But parts of the law, including provisions that could have an impact on libraries, have since come under fire.

Justice Department and FBI officials have repeatedly declined to identify how many times Patriot Act-related powers have been used to seek or obtain information from libraries, but they have strongly urged Congress not to limit their ability to do so.

The suit, originally filed under seal in Connecticut on Aug. 9, focuses on the FBI's use of a document called a "national security letter" (NSL), which allows investigators to demand records without the approval of a judge and to prohibit companies or institutions from disclosing the request. Restrictions on the FBI's use of NSLs were loosened under the Patriot Act.

The identity of the institution, the records being sought and numerous other details are edited out of the public version of the complaint released by the American Civil Liberties Union, which is a party to the lawsuit.

But the edited lawsuit reveals that the plaintiff is a member of the libraries association, that it provides "circulation and cataloging of library materials," and that it allows "library patrons . . . to search library collections and check the status of their accounts." The complaint also says the institution "provides Internet access for use by staff and patrons" and that the FBI was seeking "subscriber information, billing information and access logs" related to an unidentified target.

Justice Department spokesman Brian Rochkasse declined to comment on the dispute because of the pending litigation.

ACLU lawyer Ann Beeson said the group is asking the court to lift a gag order that has been imposed in the case and said the dispute is directly relevant to the debate on Capitol Hill over the Patriot Act.

The House and Senate approved bills in July to renew or make permanent 16 provisions of the Patriot Act set to expire at the end of the year. Civil liberties groups are particularly opposed to the House version, which, among other things, would allow those who violate a gag order in connection with an NSL to be sentenced to as long as five years in prison.

Advertisement

**RELIABLE COMMUNICATIONS  
WHEN IT  
MATTERS MOST.**

Learn more at our on-demand Webinar  
"The Facts About IP Telephony." »

**AVAYA**  
COMMUNICATIONS  
AT THE HEART OF BUSINESS

"The most immediate concern we have is that if Congress passes the House version, our client could actually go to jail for participating in the Patriot Act debate," Beeson said.

Patrice McDermott of the American Library Association said the lawsuit "shows what we've been saying all along: that the FBI is indeed very interested in libraries."

Attorney General Alberto R. Gonzales said during Senate testimony in April that the Justice Department "has no interest in rummaging through the library records or medical records of Americans" but that "libraries should not become safe havens" for terrorists or other criminals.

Gonzales said at the time that the FBI had never asked for records under a provision of the Patriot Act known by critics as the "library provision," which allows the government to demand records from a range of businesses, including libraries, in intelligence probes.

But that provision is separate from the one that governs the kind of letter used in the Connecticut case. Justice and FBI officials have repeatedly declined to say how many times such letters have been served on any kind of institution, including libraries.

Gonzales and FBI Director Robert S. Mueller III have defended the government's need to obtain records related to Internet use at public libraries. FBI investigators found that some of the Sept. 11 hijackers accessed the Internet at libraries in Florida and New Jersey.

The government is currently appealing a separate decision involving the ACLU in New York, where a federal judge ruled in September 2004 that the federal statute governing the use of national security letters was unconstitutional.

*Researcher Julie Tate contributed to this report.*

© 2005 The Washington Post Company

Advertising Links

What's this?

**Save on All Your Calls with Vonage**

When looking for local regional and long distance calling, use Vonage to make calls to all 50 states and Canada. Get voicemail, great international rates and more. Sign up today  
[www.vonage.com](http://www.vonage.com)

**MyCashNow - \$100 - \$1,500 Overnight**

Payday Loan Cash goes in your account overnight. Very low fees. Fast decisions. Direct deposit is not required. No credit check. Confidential - secure.  
[www.mycashnow.com](http://www.mycashnow.com)

**Refinance Rates Hit Record Lows**

Get \$150,000 loan for \$720 per month. Refinance while rates are low.  
[www.lowermybills.com](http://www.lowermybills.com)

**EXHIBIT D**

FBI, Using Patriot Act, Demands Library's Records - New York Times - <http://www.nytimes.com/2005/08/26/politics/26patriot.html?pagewanted=all>

**The New York Times**  
nytimes.com

August 26, 2005

## F.B.I., Using Patriot Act, Demands Library's Records

By ERIC LICHTEBLAU

WASHINGTON, Aug. 25 - Using its expanded power under the antiterrorism law known as the USA Patriot Act, the F.B.I. is demanding library records from a Connecticut institution as part of an intelligence investigation, the American Civil Liberties Union said Thursday.

The demand is the first confirmed instance in which the Federal Bureau of Investigation has used the law in this way, federal officials and the A.C.L.U. said. The government's power to demand access to library borrowing records and other material showing reading habits has been the single most divisive issue in the debate over whether Congress should extend key elements of the act after this year.

Because of federal secrecy requirements, the A.C.L.U. said it was barred from disclosing the identity of the institution or other main details of the bureau's demand, but court papers indicate that the target is a library in the Bridgeport area.

The A.C.L.U., a leading critic of the Bush administration over the Patriot Act and its antiterrorism policies, brought a lawsuit on Aug. 9 in Federal District Court in Bridgeport on behalf of the Connecticut institution. The suit was filed under seal, and names and other information were redacted in a public version it released Thursday.

The A.C.L.U. said it would seek an emergency order allowing it to discuss details of the case publicly. A hearing has been set for Wednesday in federal court in Bridgeport.

In the debate over the future of the antiterrorism law, the administration has said that it has never used the so-called library provision in the law, which falls under Section 215, to demand records from libraries or booksellers.

The A.C.L.U. said that in the Connecticut case, the bureau was using a separate investigative tool, a type of administrative subpoena known as a national security letter, to get records related to library patrons, reading materials and patrons' use of the Internet.

The bureau's power to use national security letters to demand records without a judge's approval was expanded under the antiterrorism law. Last year, a federal judge in Manhattan struck down part of the subpoena provision as unconstitutional, in part because it allowed for no judicial oversight, but the Justice Department is appealing the ruling.

Anthony D. Romero, executive director of the A.C.L.U., said the demand for the Connecticut library records "shows that our supposed hysteria over the Patriot Act wasn't so hysterical after all."

"This is a prime example of the government using its Patriot Act powers without any judicial oversight to get sensitive information on law-abiding Americans," Mr. Romero said.

Officials at the Justice Department and the F.B.I. refused comment on the issue because it involves pending litigation. But one government official, speaking on condition of anonymity because of the litigation, cautioned against reading too much into the bureau's demand for the records in Connecticut.

Because the law prevents public disclosure concerning such demands for records, the official said. "Not all the facts have come out here. But national security letters are a legitimate investigative tool, and to draw conclusions without knowing what the underlying facts are, people have to be careful about that."

The letter from the F.B.I., which was included in the lawsuit, said the material being sought was needed as part of an investigation "to protect against internal terrorism or clandestine intelligence activities." The letter warned that the recipient was prohibited "from disclosing to any person that the F.B.I. has sought or obtained access to information or records under these provisions."

The lawsuit said the Connecticut organization, which is a member of the American Library Association, "strictly guards the confidentiality and privacy of its library and Internet records, and believes it should not be forced to disclose such records without a showing of compelling need and approval by a judge."

While the antiterrorism law is still awaiting final reauthorization by Congress, both the Senate and the House moved last month to extend at least temporarily the government's power to demand library records in terrorism investigations.

Administration officials have repeatedly emphasized that they have no interest in investigating the reading habits of law-abiding Americans.

But the administration has faced strong criticism from groups like the American Library Association, which released a survey of its members in June showing that law enforcement officials had contacted libraries at least 700 times since 2001 with formal and informal inquiries about their internal records.

**EXHIBIT E**



need to justify the production of constitutionally protected information; and without specifying any means by which the recipient can contest the demand's validity. Section 2709 also permanently gags those served with NSLs from disclosing to any other person that the FBI sought or obtained information from them. Because Section 2709 was amended by the Patriot Act to remove any requirement of individualized suspicion, the FBI may now use NSLs to demand sensitive information about innocent people

2. In [REDACTED] an agent of defendant FBI served an NSL on plaintiff [REDACTED]. The NSL directed [REDACTED] to disclose certain subscriber records and other sensitive information. [REDACTED] strictly guards the confidentiality and privacy of its library and Internet records, and believes it should not be forced to disclose such records without a showing of compelling need and approval by a judge. Because the NSL gags [REDACTED] and its counsel from "disclosing to any person" that the FBI has demanded information, plaintiffs have filed this Complaint initially under seal.

3. Plaintiffs submit that Section 2709 is unconstitutional on its face and as applied. Plaintiffs further submit that the gag provision is unconstitutionally vague, overbroad, and imposes an unlawful prior restraint on speech. Plaintiffs seek a declaration that Section 2709 violates the First, Fourth, and Fifth Amendments; an injunction prohibiting the FBI from seeking to enforce the NSL served on [REDACTED] and an injunction prohibiting the FBI's further use of Section 2709 against plaintiffs or others.

#### JURISDICTION AND VENUE

4. This case arises under the United States Constitution and the laws of the United States and presents a federal question under Article III of the United States Constitution and 28

U.S.C. § 1331. The Court has authority to grant declaratory and injunctive relief pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.* The Court has authority to award costs and attorneys' fees under 28 U.S.C. § 2412. Venue is proper in this district under 28 U.S.C. § 1391(e).

PARTIES

5. Plaintiff [REDACTED]

[REDACTED] The [REDACTED] of [REDACTED] is [REDACTED]. The FBI served the NSL on [REDACTED] in his capacity as [REDACTED] of [REDACTED] sues on its own behalf and on behalf of its [REDACTED].

6. Plaintiff ACLU is a nationwide, non-profit, non-partisan organization with more than 400,000 members dedicated to the constitutional principles of liberty and equality. The ACLU is a 501(c)(4) organization. The ACLU's activities include lobbying Congress on legislation that affects civil liberties, analyzing and educating the public about such legislation, and mobilizing ACLU members and activists to lobby their legislators to protect civil rights and civil liberties. The ACLU sues on its own behalf and on behalf of its members.

7. Plaintiff ACLUF is a 501(c)(3) organization that educates the public about civil liberties and that employs lawyers who provide legal representation free of charge in cases involving civil liberties. As counsel to [REDACTED] and privy to the information contained in the NSL served on [REDACTED] lawyers employed by ACLUF are subject to Section 2709's gag provision.

8. Defendant Attorney General Alberto Gonzales heads the United States Department of Justice (DOJ), which is the agency of the United States government responsible

for enforcement of federal criminal laws and domestic intelligence investigations. Defendant Gonzales has ultimate authority for supervising all of the operations and functions of the DOJ. The DOJ includes the FBI, the agency authorized to use the law challenged in this case.

9. Defendant Robert Mueller is the Director of the FBI and is responsible for supervising all of that agency's operations. The FBI is the agency authorized to use the law challenged in this case.

10. Defendant [REDACTED] Federal Bureau of Investigation [REDACTED] Defendant [REDACTED] signed the [REDACTED] NSL.

#### STATUTORY LANGUAGE AT ISSUE

11. In its current form, as amended by the Patriot Act, Section 2709 authorizes the FBI to issue NSLs ordering "electronic communication service providers" (ECSPs) to disclose "subscriber information," "toll billing records information," and "electronic communication transactional records" upon a certification that the information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." Pub. L. 107-56, Title V, § 505(a), 115 Stat. 365 (Oct. 26, 2001) (codified as 18 U.S.C. § 2709).

12. An "electronic communication service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15).

13. Section 2709 does not require the FBI to meet a probable cause or individualized suspicion requirement of any kind before issuing an NSL.

14. Section 2709 does not require the FBI to obtain judicial authorization before issuing an NSL.

15. Section 2709 does not specify any means by which the recipient of an NSL can challenge the letter's validity.

16. Section 2709 does not require the FBI to provide prior, contemporaneous, or post-deprivation notice to an individual whose information is demanded pursuant to an NSL served on a third party, even if the information is constitutionally protected.

17. Section 2709 includes a gag provision that prohibits a person served with an NSL from disclosing to any other person that the FBI has sought or obtained records. *See* 18 U.S.C. § 2709(c) ("No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the [FBI] has sought or obtained access to information or records under this section.")

18. The gag provision, which on its face prohibits even consultation with counsel, applies in every case, whether or not the government can demonstrate a need for secrecy. *See id.*

19. The gag provision is indefinite and persists even after any legitimate need for secrecy has expired. *See id.*

20. Section 2709 is part of the Electronic Communications Privacy Act (ECPA), which Congress enacted in 1986. *See* Pub. L. 99-508, Title II, § 201[a], 100 Stat. 1867 (Oct. 21, 1986) (codified as 18 U.S.C. § 2510, *et seq.*).

21. As originally enacted, Section 2709 could be used only against people suspected of espionage. The original provision permitted the FBI to issue an NSL only if it could certify that (i) the information sought was relevant to an authorized foreign counterintelligence investigation; *and* (ii) there were specific and articulable facts giving reason to believe that the subject of the NSL was a foreign power or foreign agent. *See* 18 U.S.C. § 2709 (1988).

22. In 1993, Congress relaxed the individualized suspicion requirement. It authorized the FBI to issue an NSL if it could certify that (i) the information sought was relevant to an authorized foreign counterintelligence investigation; and (ii) there were specific and articulable facts giving reason to believe that *either* (a) the subject of the NSL was a foreign power or foreign agent, *or* (b) the subject had communicated with a person engaged in international terrorism or with a foreign agent or power "under circumstances giving reason to believe that the communication concerned international terrorism." See Pub. L. 103-142, 107 Stat. 1491 (Nov. 17, 1993).

23. In adopting the 1993 amendments, Congress recognized that "the national security letter is an extraordinary device," as it is "[e]xempt from the judicial scrutiny normally required for compulsory process." See H.Rep. 103-46 (Mar. 29, 1993).

24. In 2001, through the Patriot Act, Congress further expanded Section 2709 by deleting the individualized suspicion requirement altogether. See Pub. L. 107-56, Title V, § 505(a), 115 Stat. 365 (Oct. 26, 2001).

25. As a result of the Patriot Act, the FBI may now use NSLs to obtain sensitive information about innocent individuals who have no connection to espionage or terrorism. See 18 U.S.C. § 2709(b).

#### FACTUAL BACKGROUND

26. On [REDACTED] FBI [REDACTED] of the FBI [REDACTED] telephoned [REDACTED] to inform him that the FBI would be serving an NSL on [REDACTED] did not describe the substance of the letter, and did not notify [REDACTED] about the NSL's non-disclosure provision. [REDACTED] asked [REDACTED] who could receive service of the NSL,

and [REDACTED] told him that [REDACTED] of [REDACTED] would receive service.

27. On [REDACTED] and another [REDACTED] delivered the NSL (hereinafter [REDACTED] NSL"), a copy of which is attached hereto, to [REDACTED] of [REDACTED]. The letter, which is dated [REDACTED] is on FBI letterhead and signed by defendant [REDACTED] FBI [REDACTED] [REDACTED]

28. The [REDACTED] NSL states that [REDACTED] is "hereby directed to provide to the Federal Bureau of Investigation (FBI) any and all subscriber information, billing information and access logs of any person or entity related to the following: [REDACTED] [REDACTED]

29. The [REDACTED] NSL includes a certification that "the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."

30. The [REDACTED] NSL states, "You are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions."

31. The [REDACTED] NSL further states, "You are requested to provide records responsive to this request personally to a representative of the [REDACTED] of the FBI. Electronic versions of the records are requested, if available. Any questions you have regarding this request should be directed only to the [REDACTED]. Due to security considerations, you should neither send the records through the mail nor disclose the substance

of this request in any telephone conversation or electronic communication.” (Emphasis in original.)

32. The [REDACTED] NSL does not specify any procedure by which [REDACTED] [REDACTED] can challenge the validity of the NSL.

33. [REDACTED] told [REDACTED] that he would like to consult an attorney about the NSL, and [REDACTED] told [REDACTED] to have the attorney call him.

34. On [REDACTED] [REDACTED] called [REDACTED] to inquire about the status of [REDACTED] compliance with the NSL. [REDACTED] informed [REDACTED] that [REDACTED] had retained counsel and to direct further inquiries to counsel.

35. Section 2709 authorizes the FBI to use NSLs to demand information from a variety of for-profit and not-for-profit entities that qualify as “electronic communication service providers” because they facilitate access to the Internet and other online services for subscribers, clients, or members. Such entities include not only what are commonly known as “Internet service providers,” but also universities, businesses, public interest organizations, and public libraries.

36. Electronic communication service providers (“communication providers”) maintain a range of sensitive information about their clients.

37. Communication providers who provide clients with access to the Internet maintain information that may include the client’s name, address, e-mail addresses, telephone numbers, billing information, web sites visited, e-mail addresses with which the client has corresponded, or a list of web purchases.

38. Many people who communicate over the Internet do so anonymously or pseudonymously. Those Internet speakers who prefer to communicate anonymously are

motivated by a variety of concerns. They may prefer anonymity because they fear retaliation or reprisal; because the subjects they discuss are embarrassing, sensitive, or controversial; because they do not want to disclose personal facts about themselves; or because they fear that readers would otherwise dismiss their speech because of their race or religion or because of some other reason unrelated to the content of the speech.

39. Many of those who engage in anonymous or pseudonymous speech on the Internet would engage in self-censorship if they were not confident that their anonymity could be preserved.

40. The vast majority of libraries around the country are "electronic communication service providers" under Section 2709 because they use online services to track circulation and cataloging of library materials, to track patron borrowing, and to provide Internet access to library patrons. As a result, libraries maintain a wide range of sensitive information about the reading habits and Internet usage of library patrons.

41. Protecting library patron privacy and confidentiality has long been an integral part of the mission of libraries. The American Library Association, the oldest and largest library association in the world, with 64,000 members, recognizes that reader privacy is essential to the exercise of free speech, free thought, and free association. In a library, the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Librarians recognize an ethical responsibility to protect the privacy of library users. The ALA opposes "any use of governmental prerogatives that lead to the intimidation of individuals or groups and discourages them from exercising the right of free expression guaranteed by the First Amendment." American Library Association, Policy 53.4, adopted Feb. 2, 1973.

42. ALA has emphasized that "Libraries are one of the great bulwarks of democracy. They are living embodiments of the First Amendment because their collections include voices of dissent as well as assent. Libraries are impartial resources providing information on all points of view, available to all persons regardless of origin, age, background, or views. The role of libraries as such a resource must not be compromised by an erosion of the privacy rights of library users." American Library Association, Policy Concerning Confidentiality of Personally Identifiable Information about Library Users, adopted June 2, 1991, amended June 30, 2004.

43. ALA passed a resolution recognizing that provisions of the Patriot Act "increase the likelihood that the activities of library users, including their use of computers to browse the Web or access e-mail, may be under government surveillance without their knowledge or consent." The resolution "opposes any use of governmental power to suppress the free and open exchange of knowledge and information to intimidate individuals exercising free inquiry," and asserts "[t]hat the American Library Association considers sections of the USA Patriot Act [to be] a present danger to the constitutional rights and privacy rights of library users." American Library Association, Resolution on the USA Patriot Act and Related Measures That Infringe on the Rights of Library Users, adopted January 29, 2003.

44. Forty-eight states, [REDACTED] have statutes that explicitly protect the confidentiality of library records. [REDACTED]

45. [REDACTED] provides a number of services to [REDACTED]. It administers an [REDACTED].

circulation and cataloging of library materials, and to track community borrowing and library usage. Library patrons search library collections and check the status of their accounts.

46. also provides Internet access for use by staff and patrons at

47. also provides

to its

48. possess a wide array of sensitive information about library patrons, including information about the reading materials borrowed by library patrons and about Internet usage by library patrons.

49. is a member of the American Library Association and abides by its policies on the confidentiality of information about library patrons.

50. Section 2709(c) has prevented from disclosing information about the NSL and this lawsuit to its

51. Section 2709(c) has prevented from disclosing information about the NSL and this lawsuit to who use its

52. Section 2709(c) has prevented from disclosing information about the NSL and this lawsuit to other libraries, library service providers, and library associations.

53. Section 2709(c) has prevented from disclosing information about the NSL and this lawsuit to the press and public.

54. Section 2709(c) has prevented [REDACTED] from disclosing information about the NSL to Congress, which is currently considering legislation to amend or make permanent Section 2709 and other provisions of the Patriot Act.

55. In part because of the secrecy surrounding the government's implementation and use of new surveillance powers, the new surveillance provisions of the Patriot Act have been the subject of extraordinary public controversy. *See, e.g.,* Loretta Waldman, *Patriot Act's Future Debated; 2 Republicans Have Different Views on Proposed Revisions*, HARTFORD COURANT, June 27, 2005, at B1; David Lightman, *Civil Liberties Watchdog Debated*, HARTFORD COURANT, July 24, 2005, at A1; *A Statute of Liberty?: Patriot Act, Designed To Protect, May Also Pry*, NEWSDAY, August 3, 2005, at A10; Eric Lichtblau, *Senator Faults Briefing on Antiterrorism Law*, N.Y. TIMES, Apr. 13, 2005, at A17; Dana Priest, *Panel Questions Patriot Act Uses*, WASH. POST, Apr. 28, 2005, at A7; *Provision in Patriot Act Is Rejected: Judge Curbs Access to Phone, Web Data*, THE BOSTON GLOBE, September 30, 2004, at A1; Editorial, *Judicial Pushback*, WASH. POST, October 11, 2004, at A22; *Hearing on the USA PATRIOT ACT Before the Senate Select Committee on Intelligence*, 109th Congress (April 27, 2005).

56. The question of whether the FBI has used Patriot Act provisions to obtain information about library patrons has been of extraordinary interest in the library community, in the media, and in Congress. *See, e.g.,* Adon M. Pallasch, *U.S. Attorney to Debate ACLU Official on Patriot Act Provision*, CHICAGO SUN TIMES, Jun. 26, 2005 at pg. 32; Eric Lichtblau, *Libraries Say Yes, Officials Do Quiz Them About Users*, N.Y. TIMES, Jun. 20, 2005 at A5; American Library Association, *Libraries and the USA Patriot Act Legislation*, at <http://www.ala.org/ala/pio/mediarelations/patriotactmedia.htm>; *Hearing on the USA PATRIOT ACT Before the Senate Select Committee on Intelligence*, 109th Congress (April 27, 2005).

57. Notwithstanding widespread public concern about the Patriot Act, the Department of Justice has released very little information about the implementation and use of new surveillance powers.

58. The Department of Justice has refused to disclose aggregate statistics indicating the number of times that new surveillance provisions, including Section 2709, have been used since the passage of the Patriot Act.

59. In response to a Freedom of Information Act request submitted by the ACLU and other organizations in August 2002, the FBI released a document titled "Transactional Records NSLs Since 10/26/2001," which appears to list the ECPA NSLs issued between October 26, 2001, and January 21, 2003. The five-page list is almost entirely redacted.

60. In the past few years, one of the core priorities of the ACLU and the ACLUF has been to stem the backlash on civil liberties that has taken place in the name of national security. In particular, the ACLU and the ACLUF have been the leading voice of opposition to certain provisions of the Patriot Act.

61. The ACLU has lobbied Congress to repeal or amend parts of the Patriot Act and has worked with community groups around the country to pass more than three hundred local and seven state-wide resolutions opposing the Patriot Act.

62. The ACLUF has also litigated a number of cases involving the Patriot Act. The ACLU filed two lawsuits under the Freedom of Information Act to obtain information about the government's use of the Patriot Act. The ACLU, ACLUF, and a John Doe plaintiff also successfully challenged Section 2709 in another lawsuit, which is currently pending before the Second Circuit Court of Appeals. In federal district court in Michigan, the ACLUF represents plaintiffs in a pending facial challenge to the constitutionality of Section 215 of the Patriot Act,

another provision that allows the FBI to demand personal records or things without first establishing probable cause or providing any opportunity to challenge the demand before compliance. In addition, the ACLU filed an amicus brief in the first case ever considered by the Foreign Intelligence Surveillance Court of Review, arguing that the Patriot Act's expansion of the FBI's intelligence wiretap authority is unconstitutional.

63. Through public education, litigation, and lobbying efforts, the ACLU and the ACLUF have played a critical role in influencing the public debate over the Patriot Act. Americans around the country are actively opposing the Patriot Act by lobbying their local, state, and federal legislators. Members of Congress have now introduced numerous bills to amend provisions of the Patriot Act.

64. Section 2709(c) has prevented the ACLU and the ACLUF from disclosing information about the ██████████ NSL and about this lawsuit to the press and public.

65. Section 2709(c) has prevented the ACLU and the ACLUF from disclosing information about the ██████████ NSL to Congress, which is currently considering legislation to amend or make permanent Section 2709 and other provisions of the Patriot Act.

66. The disclosure of information about the government's use of Section 2709, particularly its use against a ██████████ would inform and influence the public and congressional debate about the Patriot Act.

67. On September 28, 2004, a federal court in New York ruled that Section 2709 violated the First and Fourth Amendments, and enjoined the FBI from issuing National Security Letters under Section 2709, or from enforcing the gag provisions of Section 2709(c). *Doe v. Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004). The court stayed enforcement of its judgment pending appeal. The case is currently on appeal to the Second Circuit Court of Appeals.

**CAUSES OF ACTION**

68. Section 2709 violates the First Amendment, on its face and as applied, by categorically and permanently prohibiting any person from disclosing to any other person that the FBI has sought or obtained information with an NSL.

69. Section 2709 violates the First Amendment, on its face and as applied, by authorizing the FBI to order the disclosure of constitutionally protected information without demonstrating a compelling need for the information or tailoring the demand to the need.

70. Section 2709 violates the First and Fourth Amendments, on its face and as applied, by failing to specify any mechanism through which the recipient of an NSL can challenge the letter's validity.

71. Section 2709 violates the First, Fourth, and Fifth Amendments, on its face and as applied, by authorizing the FBI to order the disclosure of constitutionally protected information without providing prior notice to individuals whose information is disclosed or requiring the government to justify the non-provision of notice on a case-by-case basis.

72. Section 2709 violates the Fifth Amendment, on its face and as applied, because it is unconstitutionally vague.

**PRAYER FOR RELIEF**

WHEREFORE Plaintiffs respectfully request that the Court:

1. Declare that Section 2709 violates the First, Fourth, and Fifth Amendments to the United States Constitution.
2. Permanently enjoin defendants from seeking to enforce the [REDACTED] NSL or from penalizing plaintiffs for failing to comply with it.

3. Permanently enjoin defendants from using Section 2709 against plaintiffs or any other person or entity.
4. Award plaintiffs fees and costs.
5. Grant such other and further relief as the Court deems just and proper.

Respectfully submitted,

ANNETTE M. LAMOREAUX  
*Local Counsel*  
(Connecticut Bar # 25769)  
American Civil Liberties Union of  
Connecticut Foundation  
32 Grand St.  
Hartford CT 06106  
Ph: (860) 247-9823  
Fax: (860) 728-0287  
E-mail: annettel@cclu.org

ANN BEESON  
*Lead Attorney*  
JAMEEL JAFFER  
MELISSA GOODMAN  
American Civil Liberties Union  
Foundation  
National Legal Department  
125 Broad Street, 18th Floor  
New York, NY 10004  
Ph: (212) 549-2500  
Fax: (212) 549-2651  
E-mail: annb@aclu.org

August 8, 2005