

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X
[REDACTED]
AMERICAN CIVIL LIBERTIES UNION;
and AMERICAN CIVIL LIBERTIES UNION
FOUNDATION,

Plaintiffs,

v.

JOHN ASHCROFT, 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; and MARION E.
BOWMAN, in his official capacity
as Senior Counsel to the Federal
Bureau of Investigation,

Defendants.
-----X

FILED UNDER SEAL

DECLARATION OF
DAVID W. SZADY

04 Civ. 2614 (VM)

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 motion to dismiss the complaint or for summary judgment in its favor 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).¹

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

¹ 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 prescribes or proscribes certain techniques that may or may not be used to collect intelligence information.

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 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. 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.

12. 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

13. 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.

14. 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.

15. 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.

16. 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

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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

forges 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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. For example, if a particular communication service provider discloses that it received an NSL without naming the specific subject of the inquiry, that disclosure may not, on its own, appear sensitive. However, a terrorist or foreign intelligence organization could keep track of how often particular providers receive NSLs, and could instruct its agents not to use providers most likely to receive inquiries.

28. 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

29. 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 NSLs continues.

30. 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.

31. 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

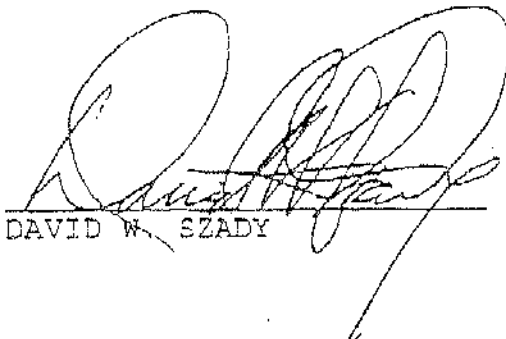
ensure that co-conspirators do not learn that the FBI is aware of the fact that they communicated with the person about whom information was sought through the NSL.

32. 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.

33. 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 NSLs - 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.

Dated: Washington, D.C.
June 24, 2004



DAVID W. SZADY