EXHIBIT B

STUART F. DELERY
Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
tony.coppolino@usdoj.gov
JAMES J. GILLIGAN
Special Litigation Counsel
james.gilligan@usdoj.gov
MARCIA BERMAN
Senior Trial Counsel
marcia.berman@usdoj.gov
BRYAN W. DEARINGER
Trial Attorney
bryan.dearinger@usdoj.gov
RODNEY PATTON
Trial Attorney
rodney.patton@usdoj.gov
U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW, Rm. 7132
Washington, D.C. 20001
Phone: (202) 514-2205; Fax: (202) 616-8470

Attorneys for the Government Defs. in their Official Capacity

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

FIRST UNITARIAN CHURCH OF LOS ANGELES, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Case No. 3:13-cv-03287-JSW **DECLARATION OF ACTING ASSISTANT DIRECTOR JOSHUA SKULE, FEDERAL BUREAU OF INVESTIGATION**

I, Joshua Skule, hereby state and declare as follows:

1. I am the Acting Assistant Director of the Counterterrorism Division, Federal Bureau of Investigation (FBI), United States Department of Justice, a component of an Executive Department of the United States Government. I am responsible for, among other things, directing and overseeing the conduct of investigations originating from the FBI's

Counterterrorism Division. As Acting Assistant Director, I have official supervision and control over files and records of the Counterterrorism Division, FBI, Washington, D.C.

2. The FBI submits this declaration in the above-captioned case in support of the Government's opposition to the plaintiffs' motion for partial summary judgment. The statements made herein are based on my personal knowledge, and information I have obtained in the course of carrying out my duties and responsibilities as Acting Assistant Director.

3. I discuss herein the National Security Agency's (NSA's) telephony metadata program, authorized by the Foreign Intelligence Surveillance Court (FISC) pursuant to Section 215 of the USA-PATRIOT Act, under which the NSA obtains and queries bulk telephony metadata for counterterrorism purposes. I address in unclassified terms the value of this program as a tool, including as a complement to other classified and unclassified FBI investigatory capabilities not discussed herein, for protecting the United States and its people from terrorist attack.

Overview of the NSA Telephony Metadata Program

4. One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. It is imperative that the United States Government have the capability to rapidly identify any terrorist threat inside the United States. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in this effort.

5. One method that the NSA has developed to accomplish this objective is the FISC-authorized bulk collection and analysis of telephony metadata that principally pertains to telephone calls to, from, or within the United States. Under the NSA's telephony metadata program authorized by the FISC, the term "metadata" refers to information that is about telephone calls but does not include cell site location information or the content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer. Specifically, such telephony metadata include comprehensive communications routing information, including but not limited to session

identifying information *(e.g.,* originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. By analyzing telephony metadata based on telephone numbers (or other identifiers) associated with terrorist operatives or activity, NSA analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the United States. The NSA telephony metadata program was specifically developed to assist the Government in detecting communications between known or suspected terrorists who are operating outside of the United States and who are in contact with others inside the United States, as well as communications between operatives within the United States.

6. Under the NSA telephony metadata program at issue in this case, the FBI obtains orders from the FISC directing certain telecommunications service providers to produce telephony metadata, also referred to as call detail records, to the NSA. The NSA then stores, queries, and analyzes the metadata for counterterrorism purposes. The FISC issues these orders under the "business records" provision of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1861, enacted by section 215 of the USA PATRIOT Act (Section 215). Under the terms of the FISC's orders, the authority to continue the program must be renewed every 90 days. The FISC first authorized the program in May 2006, and since then it has periodically renewed the program thirty-four (34) times under orders issued by fifteen (15) different FISC judges.

7. Under the FISC's orders, the information produced to the NSA is strictly limited to telephony metadata, including the telephone numbers used to make and receive the call, when the call took place, and how long the call lasted. The metadata obtained under this FISC-authorized program do not include any information about the content of those calls. The Government cannot, through this program, listen to or record any telephone conversations. The metadata principally pertain to telephone calls made from foreign countries to the United States, calls made from the United States to foreign countries, and calls within the United States.

8. Telephony metadata can be an important tool in a counter-terrorism investigation because analysis of the data permits the Government to determine quickly whether known or suspected terrorist operatives have been in contact with other persons who may be engaged in terrorist activities, including persons and activities within the United States. The NSA Section 215 telephony metadata program is carefully limited to this purpose: it is not lawful for anyone to query the bulk telephony metadata for any purpose other than counterterrorism, and FISC - imposed rules strictly limit all such queries. The program includes a variety of oversight mechanisms to prevent misuse, as well as external reporting requirements to the FISC and the United States Congress.

9. The utility of analyzing telephony metadata as an intelligence tool is not a matter of conjecture. Pen-register and trap-and-trace (PR/TT) devices provide no historical contact information, only a record of contacts with the target occurring after the devices have been installed. For decades reaching back to the Cold-War era, the FBI has relied on contact chaining as a method of detecting foreign espionage networks and operatives, both in the United States and abroad, and disrupting their plans. As discussed below, experience has shown that NSA metadata analysis, in complement with other FBI investigatory and analytical capabilities, produces information pertinent to FBI counter-terrorism investigations, and can contribute to the prevention of terrorist attacks. Indeed, in March 2009, the FISC ordered that the continued collection and retention of such metadata be justified by the submission of an affidavit from the Director of the FBI articulating the value of the program. The FBI provided the declaration as ordered and the Court reauthorized the program.

Court Approval

10. Under the Section 215 program at issue, the FBI submits an application to the FISC seeking orders directing named telecommunications service providers to produce to NSA call detail records created in the ordinary course of business. As required by Section 215, the Government's application contains a statement of facts showing that there are reasonable grounds to believe the records sought are relevant to the FBI's authorized investigations of the specified foreign terrorist organizations. In addition, the application explains that the records are

sought for investigations to protect against international terrorism, conducted under guidelines approved by the Attorney General pursuant to Executive Order 12333 (as amended) that concern specified foreign terrorist organizations. The application is supported by a declaration from a senior official of NSA's Signals Intelligence Directorate (SID).

11. Starting in May 2006 fifteen (15) separate judges of the FISC have granted the Government's applications for bulk production of telephony metadata under this program on thirty-five (35) separate occasions. From time to time, prior to granting the Government's application the Court convenes a hearing to receive additional evidence and testimony regarding the program and its implementation (as occurred in connection with the most recent renewal of the program on July 19, 2013). On granting an application, the FISC issues a "Primary Order" that recites the court's findings, including that there are reasonable grounds to believe the call detail records sought are relevant to authorized FBI investigations to protect against international terrorism. The Primary Order then provides that certain telecommunications service providers, upon receipt of appropriate Secondary Orders (discussed below), shall produce to NSA on an ongoing daily basis for the duration of the Primary Order electronic copies of the call detail records created by them containing the "telephony metadata" discussed above, explicitly excluding the substantive content of any communication, the name, address, or financial information of a subscriber or customer, and cell site location information.

12. The Primary Order also sets a specific date and time on which the NSA's authority to collect bulk telephony metadata from the providers expires, usually within 90 days of the date on which the FISC issues the order, necessitating the submission of an application for additional orders to renew the NSA's authority if the program is to continue.

13. In conjunction with the Primary Order, the FISC also issues a so-called "Secondary Order" to each of the telecommunications service providers identified in the Primary Order. These orders direct the providers, consistent with the Primary Order, to produce "telephony metadata" to NSA on an ongoing daily basis thereafter for the duration of the Order. Telephony metadata is defined under the Secondary Orders to include (and exclude) the same information as under the Primary Order.

14. These prospective orders for the production of metadata make for efficient administration of the process for all parties involved—the FISC, the Government, and the providers. In theory the FBI could seek a new set of orders on a daily basis for the records created within the preceding 24 hours. But the creation and processing of such requests would impose entirely unnecessary burdens on both the FISC and the FBI – no new information would be anticipated in such a short period of time to alter the basis of the FBI's request or the facts upon which the FISC has based its orders. Providers would also be forced to review daily requests, rather than merely continuing to comply with one ongoing request, a situation that would be more onerous on the providers and raise potential and unnecessary compliance issues. The prospective orders sought and obtained by the FBI merely ensure that the records can be sought in a reasonable manner for a reasonable period of time (90 days) while avoiding unreasonable and burdensome paperwork.

NSA's Query and Analysis of the Metadata and Dissemination of the Results

15. Under the FISC Orders at issue, before NSA may query the metadata acquired under the FISC's orders for intelligence purposes, authorized NSA officials must determine that the identifiers on which the queries will be based are reasonably suspected of being associated with one (or more) of the foreign terrorist organizations specified in the Primary Order.

16. The information on which such determinations of "reasonable, articulable suspicion" are based comes from several sources, including the FBI. The FBI, based on information acquired in the course of one or more counter-terrorism investigations, may develop reasons for concluding that a particular identifier, such as a foreign telephone number, is associated with a person (located in the United States or abroad) who is affiliated with one of the specified terrorist organizations. On that basis, the FBI may submit a request to NSA for further information about that identifier available from the collected telephony metadata.

Investigative Value of Telephony Metadata to the FBI's Counter-Terrorism Mission

17. Counter-terrorism investigations serve important purposes beyond the ambit of routine criminal inquiries and prosecution, which ordinarily focus retrospectively on specific crimes that have already occurred and the persons known or suspected to have committed them.

The key purpose of terrorism investigations, in contrast, is to prevent terrorist attacks before they occur. Terrorism investigations also provide the basis for, and inform decisions concerning, other measures needed to protect the national security, including: excluding or removing persons involved in terrorism from the United States; freezing assets of organizations that engage in or support terrorism; securing targets of terrorism; providing threat information and warnings to other federal, state, local, and private agencies and entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism threats.

18. As a result, national security investigations often have remarkable breadth, spanning long periods of time and multiple geographic regions to identify terrorist groups, their members, and their intended targets, plans, and means of attack, many of which are often unknown to the intelligence community at the outset. National security investigations thus require correspondingly far-reaching means of information-gathering to shed light on suspected terrorist organizations, their size and composition, geographic reach, relation to foreign powers, financial resources, past acts, goals, plans, and capacity for carrying them out, so that their plans may be thwarted before terrorist attacks are launched. Contact chaining information derived from queries and analysis of the Section 215 bulk telephony metadata has contributed to achieving this critical objective.

19. The FBI derives significant value from the advantages of telephony metadata analysis. The FBI is charged with collecting intelligence and conducting investigations to detect, disrupt, and prevent terrorist threats to national security. The more pertinent information the FBI has regarding such threats, the more likely it will be able to protect against them. The oft-used metaphor is that the FBI is responsible for "connecting the dots" to form a picture of the threats to national security. Information gleaned from analysis of bulk telephony metadata provides additional "dots" that the FBI uses to ascertain the nature and extent of domestic threats to the national security.

20. The NSA provides “tips” to the FBI regarding certain telephone numbers resulting from a query of the Section 215 telephony metadata. In certain instances, the FBI has received metadata-based tips containing information not previously known to the FBI about

domestic telephone numbers utilized by targets of pending preliminary investigations. The information from the metadata tips has provided articulable factual bases to believe that the subjects posed a threat to the national security such that the preliminary investigations could be converted to full investigations, which, in turn, led the FBI to focus resources on those targets and their activities. The FBI has also re-opened previously closed investigations based on information contained in metadata tips. In those instances, the FBI had previously exhausted all leads and concluded that no further investigation was warranted. The new information from the metadata tips was significant enough to warrant the re-opening of the investigations.

21. In other situations, the FBI may already have an investigative interest in a particular domestic telephone number prior to receiving a metadata tip from NSA. Nevertheless, the tip may be valuable if it provides new information regarding the domestic telephone number that re-vitalizes the investigation, or otherwise allows the FBI to focus its resources more efficiently and effectively on individuals who present genuine threats (by helping either to confirm or to rule out particular individuals as subjects for further investigation).

22. Accordingly, the NSA telephony metadata program authorized under Section 215 is a valuable source of intelligence for the FBI that is relevant to FBI-authorized international terrorism investigations.

23. The tips or leads the FBI receives from bulk metadata analysis under this program can also act as an early warning of a possible threat to the national security. The sooner the FBI obtains information about particular threats to national security, the more likely it will be able to prevent and protect against them. Bulk metadata analysis sometimes provides information earlier than the FBI's other investigative methods and techniques. In those instances, the Section 215 NSA telephony metadata program acts as an "early warning system" of potential threats against national security. Earlier receipt of this information may advance an investigation and contribute to the FBI preventing a terrorist attack that, absent the metadata tip, the FBI could not.

24. A number of recent episodes illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack. In January 2009, using authorized collection under Section 702 of the Foreign Intelligence Surveillance Act to monitor the

communications of an extremist overseas with ties to al-Qa'ida, NSA discovered a connection with an individual based in Kansas City. NSA tipped the information to the FBI, which during the course of its investigation discovered that there had been a plot in its early stages to attack the New York Stock Exchange. After further investigation, NSA queried the telephony metadata to ensure that all potential connections were identified, which assisted the FBI in running down leads. As a result of the investigation, three defendants pled guilty and were convicted of terrorism offenses relating to their efforts to support al-Qa'ida.

25. In October 2009, David Coleman Headley, a Chicago businessman and dual U.S. and Pakistani citizen, was arrested by the FBI as he tried to depart from Chicago O'Hare airport on a trip to Pakistan. At the time of his arrest, Headley and his colleagues, at the behest of al-Qa'ida, were plotting to attack the Danish newspaper that published cartoons depicting the Prophet Mohammed. Headley was later charged with support to terrorism based on his involvement in the planning and reconnaissance for the 2008 hotel attack in Mumbai. Collection against foreign terrorists and telephony metadata analysis were utilized in tandem with FBI law enforcement authorities to establish Headley's foreign ties and put them in context with his U.S. based planning efforts.

26. In September 2009, using authorized collection under Section 702 to monitor al-Qa'ida terrorists overseas, NSA discovered that one of the al-Qa'ida associated terrorists was in contact with an unknown person located in the U.S. about efforts to procure explosive material. NSA immediately tipped this information to the FBI, which investigated further, and identified the al-Qa'ida contact as Colorado-based extremist Najibullah Zazi. NSA and FBI worked together to determine the extent of Zazi's relationship with al-Qa'ida and to identify any other foreign or domestic terrorist links. NSA received Zazi's telephone number from the FBI and ran it against the Section 215 telephony metadata, identifying and passing additional leads back to the FBI for investigation. One of these leads revealed a previously unknown number for co-conspirator Adis Medunjanin and corroborated his connection to Zazi as well as to other U.S.-based extremists. Zazi and his co-conspirators were subsequently arrested. Upon indictment,

Zazi pled guilty to conspiring to bomb the New York City subway system. In November 2012, Medunjanin was sentenced to life in prison.

Alternatives to the NSA's Bulk Collection of Telephony Metadata

27. The NSA bulk collection program at issue here presents distinct advantages. The contact chaining capabilities offered by the program exceed the chaining that is performed on data collected pursuant to other means, including traditional means of case-by-case intelligence gathering targeted at individual telephone numbers such as subpoena, warrant, national security letter, pen-register and trap-and-trace (PR/TT) devices, or more narrowly defined orders under Section 215. This is so in at least two important respects, namely, the NSA's querying and analysis of the aggregated bulk telephony metadata under this program.

28. First, the agility of querying the metadata collected by NSA under this program allows for more immediate contact chaining, which is significant in time-sensitive situations of suspects' communications with known or as-yet unknown co-conspirators. For example, if investigators find a new telephone number when an agent of one of the identified international terrorist organizations is captured, and the Government issues a national security letter for the call detail records for that particular number, it would only be able to obtain the first tier of telephone number contacts and, in rare instances, the second tier of contacts if the FBI separately demonstrates the relevance of the second-generation information to the national security investigation. At least with respect to the vast majority of national security letters issued, new national security letters would have to be issued for telephone numbers identified in the first tier, in order to find an additional tier of contacts. The delay inherent in issuing new national security letters would necessarily mean losing valuable time.

29. Second, aggregating the NSA telephony metadata from different telecommunications providers enhances and expedites the ability to identify chains of communications across multiple providers. Furthermore, NSA disseminations provided to the FBI from this program may include NSA's analysis informed by its unique collection capabilities.

Conclusion

30. As I explained above, the principal objective of FBI counter-terrorism investigations is to prevent and protect against potentially catastrophic terrorist attacks on the U.S. homeland and its people before they occur. In each instance, success depends on detecting and developing a sufficiently clear and complete picture of a terrorist network and its activities in time to thwart its plans. The exploitation of terrorist communications is a tool in this effort, and NSA's analysis of bulk telephony metadata under this FISC-authorized program provides the Government with one means of discovering communications involving unknown terrorist operatives.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on December 5, 2013

Joshua Skule
Acting Assistant Director
Counterterrorism Division
Federal Bureau of Investigation
Washington, D.C.