UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION, Plaintiffs, v. JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; CHARLES T. HAGEL, in his official capacity as Secretary of Defense; ERIC H. HOLDER, in his official capacity as Attorney General of the United States; and JAMES B. COMEY, in his official capacity as Director of the Federal Bureau of Investigation, Defendants.	13 Civ. 3994 (WHP) ECF Case

DECLARATION OF TERESA H. SHEA, SIGNALS INTELLIGENCE DIRECTOR NATIONAL SECURITY AGENCY

I, Teresa H. Shea, do hereby state and declare as follows:

(U) Introduction and Summary

1. I am the Director of the Signals Intelligence Directorate (SID) at the National Security Agency (NSA), an intelligence agency within the Department of Defense (DoD). I am responsible for, among other things, protecting NSA Signals Intelligence activities, sources, and methods against unauthorized disclosures. Under Executive Order No. 12333, 46 Fed. Reg. 59941 (1981), as amended on January 23, 2003, 68 Fed. Reg. 4075 (2003), and August 27, 2004, 69 Fed. Reg. 53593 (2004), and August 4, 2008, 73 Fed. Reg. 45325, the NSA is responsible for the collection, processing, and dissemination of Signals Intelligence (SIGINT) information for

the foreign intelligence purposes of the U.S. I have been designated an original TOP SECRET classification authority under Executive Order (E.O.) 13526, 75 Fed. Reg. 707 (Jan. 5, 2010), and Department of Defense Directive No. 5200.1-R, Information Security Program Regulation, 32 C.F.R. 159a.12 (2000).

2. My statements herein are based upon my personal knowledge of SIGINT collection and NSA operations, the information available to me in my capacity as SID Director, and the advice of counsel.

3. The NSA was established by Presidential Directive in 1952 as a separately organized agency within the DOD under the direction, authority, and control of the Secretary of Defense. The NSA's foreign intelligence mission includes the responsibility to collect, process, analyze, produce, and disseminate SIGINT information for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) to support national and departmental missions. See E.O. 12333, section 1.7(c), as amended.

4. The NSA's responsibilities include SIGINT, i.e., the collection, processing and dissemination of intelligence information from certain signals for foreign intelligence and counterintelligence purposes and to support military operations, consistent with U.S. laws and the protection of privacy and civil liberties. In performing its SIGINT mission, the NSA exploits foreign electromagnetic signals, communications, and information about communications to obtain intelligence information necessary to national defense, national security, or the conduct of foreign affairs. The NSA has developed a sophisticated worldwide SIGINT collection network that acquires foreign and international electronic communications. The technological infrastructure that supports the NSA's foreign intelligence information collection network has

taken years to develop at a cost of billions of dollars and a remarkable amount of human effort. It relies on sophisticated collection and processing technology.

5. As explained below, plaintiffs' motion inaccurately describes an NSA intelligence collection program involving the acquisition and analysis of telephony metadata. While the NSA obtains telephony metadata in bulk from telecommunications service providers, the NSA's use of that data is strictly controlled; only a very small percentage of the total data collected is ever reviewed by intelligence analysts; and results of authorized queries can be further analyzed and disseminated for valid counterterrorism purposes.

OVERVIEW OF PROGRAM

6. One of the greatest challenges the U.S. 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 U.S. Detecting and preventing threats by exploiting terrorist communications has been, and continues to be, one of the tools in this effort. It is imperative that we have the capability to rapidly detect any terrorist threat inside the U.S.

7. One method that the NSA has developed to accomplish this task is analysis of metadata associated with telephone calls within, to, or from the U.S. The term "telephony metadata" or "metadata" as used here refers to data collected under the program that are about telephone calls—such as the initiating and receiving telephone numbers, and the time and duration of the calls—but does not include the substantive content of those calls or any subscriber identifying information.

8. By analyzing telephony metadata based on telephone numbers associated with terrorist activity, trained expert intelligence analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the U.S.

9. Foreign terrorist organizations use the international telephone system to communicate with one another between numerous countries all over the world, including calls to and from the U.S. When they are located inside the U.S., terrorist operatives also make domestic U.S. telephone calls. The most analytically significant terrorist-related communications are those with one end in the U.S., or those that are purely domestic, because those communications are particularly likely to identify suspects in the U.S. whose activities may include planning attacks against the homeland.

10. The telephony metadata collection program was specifically developed to assist the U.S. Government in detecting such communications between known or suspected terrorists who are operating outside of the U.S. and who are communicating with others inside the U.S., as well as communications between operatives who are located within the U.S.

11. Detecting and linking these types of communications was identified as a critical intelligence gap in the aftermath of the September 11, 2001 attacks. One striking example of this gap is that, prior to those attacks, the NSA intercepted and transcribed seven calls made by hijacker Khalid al-Mihdhar, then living in San Diego, California, to a telephone identifier associated with an al Qaeda safe house in Yemen. The NSA intercepted these calls using overseas signals intelligence capabilities, but those capabilities did not capture the calling party's telephone number identifier. Because they lacked the U.S. telephone identifier, NSA analysis mistakenly concluded that al-Mihdhar was overseas and not in California. Telephony metadata of the type acquired under this program, however, would have included the missing information

and might have permitted NSA intelligence analysts to tip FBI to the fact that al-Mihdhar was calling the Yemeni safe house from a U.S. telephone identifier.

12. The utility of analyzing telephony metadata as an intelligence tool has long been recognized. As discussed below, experience also shows that telephony metadata analysis in fact produces information pertinent to FBI counterterrorism investigations, and can contribute to the prevention of terrorist attacks.

13. Beginning in May 2006 and continuing to this day, pursuant to orders obtained from the Foreign Intelligence Surveillance Court ("FISC"), under the "business records" provision of the Foreign Intelligence Surveillance Act ("FISA"), enacted by Section 215 of the USA PATRIOT Act, codified at 50 U.S.C. § 1861 (Section 215), NSA has collected and analyzed bulk telephony metadata from telecommunications service providers to close the intelligence gap that allowed al-Mihdhar to operate undetected within the U.S. while communicating with a known terrorist overseas.

14. Pursuant to Section 215, the FBI obtains orders from the FISC directing certain telecommunications service providers to produce all business records created by them (known as call detail records) that contain information about communications between telephone numbers, generally relating to telephone calls made between the U.S. and a foreign country and calls made entirely within the U.S. By their terms, those orders must be renewed approximately every 90 days. Redacted, declassified versions of a recent FISC "Primary Order" and "Secondary Order," directing certain telecommunications service providers to produce telephony metadata records to NSA, and imposing strict conditions on the Government's access to and use and dissemination of the data, are attached, respectively, as Exhibits A and B hereto. At least 14 different FISC

judges have entered a total of 34 orders authorizing NSA's bulk collection of telephony metadata under Section 215, most recently on July 19, 2013.

15. Under the terms of the FISC's orders, the information the Government is authorized to collect includes, as to each call, the telephone numbers that placed and received the call, other session-identifying information (e.g., International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card number, and the date, time, and duration of a call. The FISC's orders authorizing the collection do not allow the Government to collect the content of any telephone call, nor the names, addresses, or financial information of parties to any call. The metadata collected by the Government pursuant to these orders also does not include cell site locational information.

16. The NSA, in turn, stores and analyzes this information under carefully controlled circumstances, and refers to the FBI information about communications (e.g., telephone numbers, dates of calls, etc.) that the NSA concludes have counterterrorism value, typically information about communications between known or suspected terrorist operatives and persons located within the U.S.

17. Under the FISC's orders, the Government is prohibited from accessing the metadata for any purpose other than obtaining counterterrorism information relating to telephone numbers (or other identifiers) that are reasonably suspected of being associated with specific foreign terrorist organizations or rendering the metadata useable to query for such counterterrorism related information.

18. Pursuant to Section 215 and the FISC's orders, the NSA does not itself in the first instance record any metadata concerning anyone's telephone calls. Nor is any non-governmental party required by Section 215, the FISC or the NSA to create or record the information that the

NSA obtains pursuant to Section 215 and FISC orders. Rather, pursuant to the FISC's orders, telecommunications service providers turn over to the NSA business records that the companies already generate and maintain for their own pre-existing business purposes (such as billing and fraud prevention).

QUERY AND ANALYSIS OF METADATA

19. Under the FISC's orders authorizing the NSA's bulk collection of telephony metadata, the NSA may access the data for purposes of obtaining counterterrorism information only through queries (term searches) using metadata "identifiers," e.g., telephone numbers, that are associated with a foreign terrorist organization.

20. Specifically, under the terms of the FISC's Primary Order, before an identifier may be used to query the database there must be a "reasonable articulable suspicion" (RAS), based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, that the identifier is associated with one of the identified international terrorist organizations that are subjects of FBI counterterrorism investigations. The RAS requirement ensures an ordered and controlled querying of the collected data; it is also designed to prevent any general browsing of data. Further, when the identifier is reasonably believed to be used by a U.S. person, the suspicion of association with a foreign terrorist organization cannot be based solely on activities protected by the First Amendment. An identifier used to commence a query of the data is referred to as a "seed."

21. Information responsive to an authorized query could include telephone numbers that have been in contact with the terrorist-associated number used to query the data, plus the dates, times, and durations of the calls. Query results do not include the identities of the individuals

associated with the responsive telephone numbers, because that is subscriber information that is not included in the telephony metadata.

22. Under the FISC's orders, the NSA may also obtain information concerning second- and third-tier contacts of the identifier, also known as "hops." The first "hop" refers to the set of identifiers directly in contact with the seed identifier. The second "hop" refers to the set of identifiers found to be in direct contact with the first "hop" identifiers, and the third "hop" refers to the set of identifiers found to be in direct contact with the second "hop" identifiers.

23. Although bulk metadata are consolidated and preserved by the NSA pursuant to Section 215, the vast majority of that information is never seen by any person. Only the tiny fraction of the telephony metadata records that are responsive to queries authorized under the RAS standard are extracted, reviewed, or disseminated by NSA intelligence analysts, and only under carefully controlled circumstances.

24. For example, although the number of unique identifiers has varied over the years, in 2012, fewer than 300 met the RAS standard and were used as seeds to query the data after meeting the standard. Because the same seed identifier can be queried more than once over time, can generate multiple responsive records, and can be used to obtain contact numbers up to three "hops" from the seed identifier, the number of metadata records responsive to such queries is substantially larger than 300, but it is still a very small percentage of the total volume of metadata records.

25. There is no typical number of records responsive to a query of the metadata—the number varies widely depending on how many separate telephone numbers (or other identifiers)

the "seed" identifier has been in direct contact with, how many separate identifiers those in the first-tier contact, and so forth.[1]

26. The NSA does not disseminate metadata information that it has not determined to be of counterterrorism value, regardless of whether it was obtained at the first, second, or third hop from a seed identifier. Rather, NSA intelligence analysts work to ascertain which of the results are likely to contain foreign intelligence information, related to counterterrorism, that would be of investigative value to the FBI (or other intelligence agencies). For example, analysts may rely on SIGINT or other intelligence information available to them, or chain contacts within the query results themselves, to inform their judgment as to what information should be passed to the FBI as leads or "tips" for further investigation. As a result, during the three-year period extending from May 2006 (when the FISC first authorized NSA's telephony metadata program under Section 215) through May 2009, NSA provided to the FBI and/or other intelligence agencies a total of 277 reports containing approximately 2,900 telephone identifiers that the NSA had identified.

27. It is not accurate, therefore, to suggest that the NSA can or does "track" or "keep track of" all Americans' calls or that it engages in "surveillance," under Section 215. Rather, by the terms of the FISC's orders, the NSA can only access metadata information within, at most,

[1] Plaintiffs' conjecture that queries using a single seed identifier could capture metadata records concerning calls by over two million people is erroneous as a matter of simple arithmetic. Assuming, as plaintiffs hypothesize, that an individual or individuals associated with a "seed" telephone number made calls to or received calls from 40 other telephone numbers, the first "hop" of a query based on that number would return metadata information on those 40 telephone numbers. At the second "hop," if each of those 40 numbers made contact with 40 other numbers (none of which overlapped, a questionable assumption), the query would return information about 1600 numbers. If in turn each of those 1600 numbers placed calls to or received calls from 40 non-overlapping numbers, a third-hop would yield information on a total of 64,000 numbers. Only if the FISC's orders permitted NSA to review the metadata of contacts at the fourth "hop" from a seed identifier, which they do not, could the number exceed 2 million (40 times 64,000).

three "hops" of an approved seed identifier that is reasonably suspected of being associated with a foreign terrorist organization specified in the FISC's orders.

28. Even when the NSA conducts authorized queries of the database, it does not use the results to provide the FBI, or any other agency, with complete profiles on suspected terrorists or comprehensive records of their associations. Rather, the NSA applies the tools of SIGINT analysis to focus only on those identifiers which, based on the NSA's experience and judgment, and other intelligence available to it, may be of use to the FBI in detecting persons in the U.S. who may be associated with a specified foreign terrorist organization and acting in furtherance of their goals. Indeed, under the FISC's orders, the NSA is prohibited from disseminating any U.S.-person information derived from the metadata unless one of a very limited number of senior NSA officials determines that the information is in fact related to counterterrorism information, and is necessary to understand the counterterrorism information or assess its importance. The NSA disseminates no information derived from the metadata about persons whose identifiers have not been authorized as query terms under the RAS standard, or whose metadata are not responsive to other queries authorized under that standard.

MINIMIZATION PROCEDURES AND OVERSIGHT

29. The NSA's access to, review, and dissemination of telephony metadata collected under Section 215 is subject to rigorous procedural, technical, and legal controls, and receives intensive oversight from numerous sources, including frequent internal NSA audits, Justice Department and Office of the Director of National Intelligence (ODNI) oversight, and reports to the FISC and to the Congressional intelligence committees.

30. In accordance with the requirements of Section 215, "minimization procedures" are in place to guard against inappropriate or unauthorized dissemination of information relating to

U.S. persons. First among these procedures is the requirement that the NSA store and process the metadata in repositories within secure networks, and that access to the metadata be permitted only for purposes allowed under the FISC's order, specifically database management and authorized queries for counterterrorism purposes under the RAS standard. In addition, the metadata must be destroyed no later than five years after their initial collection.

31. Second, under the FISC's orders no one other than twenty-two designated officials in the NSA's Homeland Security Analysis Center and the Signals Intelligence Directorate can make findings of RAS that a proposed seed identifier is associated with a specified foreign terrorist organization. For identifiers believed to be associated with U.S. persons, the NSA's Office of General Counsel must also determine that a finding of RAS is not based solely on activities protected by the First Amendment. And, as noted above, the minimization requirements also limit the results of approved queries to metadata within three hops of the seed identifier.

32. Third, while the results of authorized queries of the metadata may be shared, without minimization, among trained NSA personnel for analysis purposes, no results may be disseminated outside of the NSA except in accordance with the minimization and dissemination requirements and established NSA procedures. Moreover, prior to dissemination of any U.S.-person information outside of the NSA, one of a very limited number of NSA officials must determine that the information is in fact related to counterterrorism information, and is necessary to understand the counterterrorism information or assess its importance.

33. Fourth, in accordance with the FISC's orders, the NSA has imposed stringent and mutually reinforcing technological and personnel training measures to ensure that queries will be made only as to identifiers about which RAS has been established. These include requirements that intelligence analysts receive comprehensive training on the minimization procedures

applicable to the use, handling, and dissemination of the metadata, and technical controls that prevent NSA intelligence analysts from seeing any metadata unless as the result of a query using an approved identifier.

34. Fifth, the telephony metadata collection program is subject to an extensive regime of oversight and internal checks and is monitored by the Department of Justice (DOJ), the FISC, and Congress, as well as the Intelligence Community. Among these additional safeguards and requirements are audits and reviews of various aspects of the program, including RAS findings, by several entities within the Executive Branch, including the NSA's legal and oversight offices and the Office of the Inspector General, as well as attorneys from DOJ's National Security Division and the Office of the Director of National Intelligence.

35. Finally, in addition to internal oversight, any compliance matters in the program identified by the NSA, DOJ, or ODNI are reported to the FISC. Applications for 90-day renewals must report information on how the NSA's authority to collect, store, query, review and disseminate telephony metadata was implemented under the prior authorization. Significant compliance incidents are also reported to the Intelligence and Judiciary Committees of both houses of Congress.

COMPLIANCE INCIDENTS

36. Since the telephony metadata collection program under Section 215 was initiated, there have been a number of significant compliance and implementation issues (described below) that were discovered as a result of internal NSA oversight and of DOJ and ODNI reviews. Upon discovery, these violations were reported by the Government to the FISC and Congress, the NSA remedied the problems, and the FISC reauthorized the program.

37. For example, beginning in mid-January 2009, the Government notified the FISC that the NSA employed an "alert list" consisting of counterterrorism telephony identifiers to provide automated notification to signals intelligence analysts if one of their assigned foreign counterterrorism targets was in contact with a telephone identifier in the U.S., or if one of their targets associated with foreign counterterrorism was in contact with a foreign telephone identifier. The NSA's process compared the telephony identifiers on the alert list against incoming Section 215 telephony metadata as well as against telephony metadata that the NSA acquired pursuant to its Executive Order 12333 SIGINT authorities. Reports filed with the FISC incorrectly stated that the NSA had determined that each of the telephone identifiers it placed on the alert list were supported by facts giving rise to RAS that the telephone identifier was associated with a foreign terrorist organization as required by the FISC's orders, i.e., was RAS-approved. In fact, however, the majority of telephone identifiers included on the alert list had not gone through the process of becoming RAS approved, even though the identifiers were suspected of being associated with a foreign terrorist organization. The NSA shut down the automated alert list process and corrected the problem.

38. Following this notification, the Director of the NSA ordered an end-to-end system engineering and process review of its handling of the Section 215 metadata. On March 2, 2009, the FISC ordered the NSA to seek FISC approval to query the Section 215 metadata on a case-by-case basis, except where necessary to protect against an imminent threat to human life. The FISC further ordered the NSA to file a report with the FISC following the completion of the end-to-end review discussing the results of the review and any remedial measures taken. The report filed by the NSA discussed all of the compliance incidents, some of which involved queries of the Section 215 metadata using non-RAS approved telephone identifiers, and how they had been

remedied. The compliance incidents, while serious, generally involved human error or complex technology issues related to the NSA's compliance with particular aspects of the FISC's orders. Subsequently, the FISC required a full description of any incidents of dissemination outside of the NSA of U.S. person information in violation of court orders, an explanation of the extent to which the NSA had acquired foreign-to-foreign communications metadata pursuant to the court's orders and whether the NSA had complied with the terms of court orders in connection with any such acquisitions, and certification as to the status of several types of data to the extent those data were collected without authorization.

39. The U.S. Government completed these required reviews and reported to the FISC in August 2009. In September 2009, the FISC entered an order permitting the NSA to once again assess RAS without seeking pre-approval from the FISC subject to the minimization and other requirements that remain in place today.

40. In fact, in an August 2013 Amended Memorandum Decision discussing the Court's reasons for renewing the continued operation of the section 215 telephony metadata program for a 90-day period, the FISC stated, "The Court is aware that in prior years there have been incidents of non-compliance with respect to the NSA's handling of produced information. Through oversight by this Court over a period of months, those issues were resolved." *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, Case No. BR 13-109, Amended Memorandum Opinion at 5 n.8 (FISC, released in redacted form September 17, 2013; *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf) (last visited September 18, 2013).

41. These incidents, including the FISC's related opinions, were also reported to Congress in 2009.

42. Having received these reports and having been informed that the Government interpreted section 215 to authorize the bulk collection of telephony metadata, Congress has twice reauthorized section 215, without relevant modification, in 2010 and again in 2011.

43. In sum, the factors giving rise to compliance incidents discussed in this section have been remedied. Moreover, even the most serious incidents, in which non-RAS approved selectors were used to query the database, would not have allowed the NSA to compile the type of richly detailed profiles of Americans' lives about which plaintiffs speculate. That type of analysis is simply not possible from the raw telephony metadata that is collected under the program, as it does not identify who is calling whom and for what purpose.

BENEFITS OF METADATA COLLECTION

44. Among other benefits, the bulk collection of telephony metadata under Section 215 has animportant value to NSA intelligence analysts tasked with identifying potential terrorist threats to the U.S. homeland, in support of FBI, by enhancing their ability to detect, prioritize, and track terrorist operatives and their support networks both in the U.S. and abroad. By applying the FISC-ordered RAS standard to telephone identifiers used to query the metadata, NSA intelligence analysts are able to: (i) detect domestic identifiers calling foreign identifiers associated with one of the foreign terrorist organizations and discover identifiers that the foreign identifiers are in contact with; (ii) detect foreign identifiers associated with a foreign terrorist organization calling into the U.S. and discover which domestic identifiers are in contact with the foreign identifiers; and (iii) detect possible terrorist-related communications occurring between communicants located inside the U.S.

45. Although the NSA possesses a number of sources of information that can each be used to provide separate and independent indications of potential terrorist activity against the U.S. and its interests abroad, the best analysis occurs when NSA intelligence analysts can consider the information obtained from each of those sources together to compile and disseminate to the FBI as complete a picture as possible of a potential terrorist threat. While telephony metadata is not the sole source of information available to NSA counterterrorism personnel, it provides a component of the information NSA intelligence analysts rely upon to execute this threat identification and characterization role.

46. An advantage of bulk metadata analysis as applied to telephony metadata, which are interconnected in nature, is that it enables the Government to quickly analyze past connections and chains of communication. Unless the data is aggregated, it may not be feasible to detect chains of communications that cross communication networks. The ability to query accumulated telephony metadata significantly increases the NSA's ability to rapidly detect persons affiliated with the identified foreign terrorist organizations who might otherwise go undetected.

47. Specifically, when the NSA performs a contact-chaining query on a terrorist associated telephone identifier, it is able to detect not only the further contacts made by that first tier of contacts, but the additional tiers of contacts, out to a maximum of three "hops" from the original identifier, as authorized by the applicable FISC order. The collected metadata thus holds contact information that can be immediately accessed as new terrorist-associated telephone identifiers are identified. Multi-tiered contact chaining identifies not only the terrorist's direct associates but also indirect associates, and, therefore provides a more complete picture of those who associate with terrorists and/or are engaged in terrorist activities.

48. Another advantage of the metadata collected in this matter is that it is historical in nature, reflecting contact activity from the past. Given that terrorist operatives often lie dormant for extended periods of time, historical connections are critical to understanding a newly-identified target, and metadata may contain links that are unique, pointing to potential targets that may otherwise be missed.

49. Bulk metadata analysis under Section 215 thus enriches NSA intelligence analysts' understanding of the communications tradecraft of terrorist operatives who may be preparing to conduct attacks against the U.S. This analysis can be important considering that terrorist operatives often take affirmative and intentional steps to disguise and obscure their communications.

50. Furthermore, the Section 215 metadata program complements information that the NSA collects via other means and is valuable to NSA, in support of the FBI, for linking possible terrorist-related telephone communications that occur between communicants based solely inside the U.S.

51. As a complementary tool to other intelligence authorities, the NSA's access to telephony metadata improves the likelihood of the Government being able to detect terrorist cell contacts within the U.S. With the metadata collected under Section 215 pursuant to FISC orders, the NSA has the information necessary to perform the call chaining that enables NSA intelligence analysts to obtain a much fuller understanding of the target and, as a result, allows the NSA to provide FBI with a more complete picture of possible terrorist-related activity occurring inside the U.S.

52. The value of telephony metadata collected under Section 215 is not hypothetical. While many specific instances of the Government's use of telephony metadata under Section 215 remain classified, a number of instances have been disclosed in declassified materials.

53. An illustration of the particular value of the bulk metadata program under Section 215—and a tragic example of what can occur in its absence—is the case of 9/11 hijacker Khalid al-Mihdhar, which I have described above. The Section 215 telephony metadata collection program addresses the information gap that existed at the time of the al-Mihdhar case. It allows the NSA to rapidly and effectively note these types of suspicious contacts and, when appropriate, to tip them to the FBI for follow-on analysis or action.

54. Furthermore, once an identifier has been detected, the NSA can use bulk telephony metadata along with other data sources to quickly identify the larger network and possible co-conspirators both inside and outside the U.S. for further investigation by the FBI with the goal of preventing future terrorist attacks.

55. As the case examples in the FBI declaration accompanying the defendants' response motion demonstrates, Section 215 bulk telephony metadata is a resource not only in isolation, but also for investigating threat leads obtained from other SIGINT collection or partner agencies. This is especially true for the NSA-FBI partnership. The Section 215 telephony metadata program enables NSA intelligence analysts to evaluate potential threats that it receives from or reports to the FBI in a more complete manner than if this data source were unavailable.

56. Section 215 bulk telephony metadata complements other counterterrorist-related collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the NSA in applying limited linguistic resources available to the counterterrorism mission against links that have the highest probability of connection to terrorist targets. Put another way, while

Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA prioritize for content analysis communications of non-U.S. persons which it acquires under other authorities. Such persons are of heightened interest if they are in a communication network with persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis so that the U.S. Government gains the best possible understanding of terrorist target actions and intentions.

57. Reliance solely on traditional, case-by-case intelligence gathering methods, restricted to known terrorist identifiers, would significantly impair the NSA's ability to accomplish many of the aforementioned objectives.

58. Without the ability to obtain and analyze bulk metadata, the NSA would lose a tool for detecting communication chains that link to identifiers associated with known and suspected terrorist operatives, which can lead to the identification of previously unknown persons of interest in support of anti-terrorism efforts both within the U.S. and abroad. Having the bulk telephony metadata available to query is part of this effort, as there is no way to know in advance which numbers will be responsive to the authorized queries.

59. The bulk metadata allows retrospective analyses of prior communications of newly-discovered terrorists in an efficient and comprehensive manner. Any other means that might be used to attempt to conduct similar analyses would require multiple, time-consuming steps that would frustrate needed rapid analysis in emergent situations, and could fail to capture some data available through bulk metadata analysis.

60. If the telephony metadata are not aggregated and retained for a sufficient period of time, it will not be possible for the NSA to detect chains of communications that cross different providers and telecommunications networks. But for the NSA's metadata collection, the NSA

would need to seek telephonic records from multiple providers whenever a need to inquire arose, and each such provider may not maintain records in a format that is subject to a standardized query.

61. Thus, contrary to plaintiffs' suggestion, the Government could not achieve the aforementioned benefits of section 215 metadata collection through alternative means.

62. While plaintiffs suggest the use of more targeted inquiries—whether through a subpoena, national security letter ("NSL"), or pen register or trap-and-trace ("PR/TT") device authorized under the FISA— solely of records directly pertaining to a terrorism subject, those measures would fail to permit the comprehensive and retrospective analyses detailed above of communication chains that might, and sometimes do, reveal previously unknown persons of interest in terrorism investigations. Targeted inquiries also would fail to capture communications chains and overlaps that can be of investigatory significance, because targeted inquiries would eliminate the NSA's ability to collect and analyze metadata of communications occurring at the second and third "hop" from a terrorist suspect's initial "seed"; rather, they would only reveal communications directly involving the specific targets in question. In other words, targeted inquiries would capture only one "hop." As a result, the Government's ability to discover and analyze communications metadata revealing the fact that as-yet unknown identifiers are linked in a chain of communications with identified terrorist networks would be impaired.

63. In sum, any order barring the Government from employing the section 215 metadata collection program would deprive the Government of unique capabilities that could not be completely replicated by other means, and as a result would cause an increased risk to national security and the safety of the American public.

BURDEN OF COMPLYING WITH A PRELIMINARY INJUNCTION

64. Beyond harming national security and the Government's counterterrorism capabilities, plaintiffs' proposed preliminary injunction would seriously burden the Government. While plaintiffs seek an order barring the Government from collecting metadata reflecting their calls, the Government does not know plaintiffs' phone numbers, and would need plaintiffs to identify all numbers they use to even attempt to implement such an injunction. Ironically, as explained above, these numbers are not currently visible to NSA intelligence analysts unless they are within a three hops of a call chain of a number that based on RAS is associated with a foreign terrorist organization.

65. Even if plaintiffs' phone numbers were available, extraordinarily burdensome technical and logistical hurdles to compliance with a preliminary injunction order would remain. Technical experts would have to develop a solution such as removing the numbers from the system upon receipt of each batch of metadata or developing a capability whereby plaintiffs' numbers would be received by NSA but would not be visible in response to an authorized query. To identify, design, build, and test the best implementation solution would potentially require the creation of new full-time positions and could take six months or more to implement. Once implemented, any potential solution could undermine the results of any authorized query of a phone number that based on RAS is associated with one of the identified foreign terrorist organizations by eliminating, or cutting off potential call chains. If this Court were to grant a preliminary injunction and the defendants were to later prevail on the merits of this litigation, it could prove extremely difficult to develop a solution to reinsert any quarantined records and would likely take considerable resources and several months to build, test, and implement a re-insertion capability suited to this task.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

DATE: 10-1-13

Teresa H. Shea
Signals Intelligence Director
National Security Agency