14-42

IN THE

United States Court of Appeals

FOR THE

Second Circuit

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs–Appellants,

– 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–Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

JOINT APPENDIX

Volume 2 of 2 (JA258–JA394)

Christopher T. Dunn
Arthur N. Eisenburg
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004
Phone: (212) 607-3300
Fax: (212) 607-3318
aeisenberg@nyclu.org

Jameel Jaffer
Alex Abdo
Patrick Toomey
Brett Max Kaufman
Catherine Crump
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
jjaffer@aclu.org

JOINT APPENDIX

VOLUME TWO

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

Exhibit A

~~TOP SECRET//SI//NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket Number: BR

13-80

PRIMARY ORDER

A verified application having been made by the Director of the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, requiring the

~~TOP SECRET//SI//NOFORN~~

Derived from: ~~Pleadings in the above-captioned docket~~
Declassify on: ~~12 April 2038~~

production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:

1. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things. [50 U.S.C. § 1861(c)(2)(D)]

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number [redacted] and its predecessors. [50 U.S.C. § 1861(c)(1)]

~~TOP SECRET//SI//NOFORN~~

Accordingly, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application is GRANTED, and it is

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata"[1] created by [redacted]

B. The Custodian of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis

[1] For purposes of this Order "telephony metadata" includes 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. Telephony metadata does not include the substantive 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.

~~TOP SECRET//SI//NOFORN~~

thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by [redacted] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [redacted]

(2) With respect to any information the FBI receives as a result of this Order (information that is disseminated to it by NSA), the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General's Guidelines for Domestic FBI Operations* (September 29, 2008).

(3) With respect to the information that NSA receives as a result of this Order, NSA shall strictly adhere to the following minimization procedures:

A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors ("BR metadata") for any purpose except as described herein.

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA's control.[2] The BR metadata shall carry unique markings such

[2] The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA shall ensure that any access

~~TOP SECRET//SI//NOFORN~~

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.[3] Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms[4] that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes,

---

or use of the BR metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

[3] The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA, will not receive special training regarding the authority granted herein.

[redacted]

~~TOP SECRET//SI//NOFORN~~

but the results of any such queries will not be used for intelligence analysis purposes. An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

C. NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through contact chaining queries of the BR metadata as described in paragraph 17 of the Declaration of [redacted], attached to the application as Exhibit A, using selection terms approved as "seeds" pursuant to the RAS approval process described below.[5] NSA shall ensure, through adequate and

[5] For purposes of this Order, "National Security Agency" and "NSA personnel" are defined as any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to FISA if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). NSA personnel shall not disseminate BR metadata outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of this Order that are applicable to the NSA.

appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.[6]

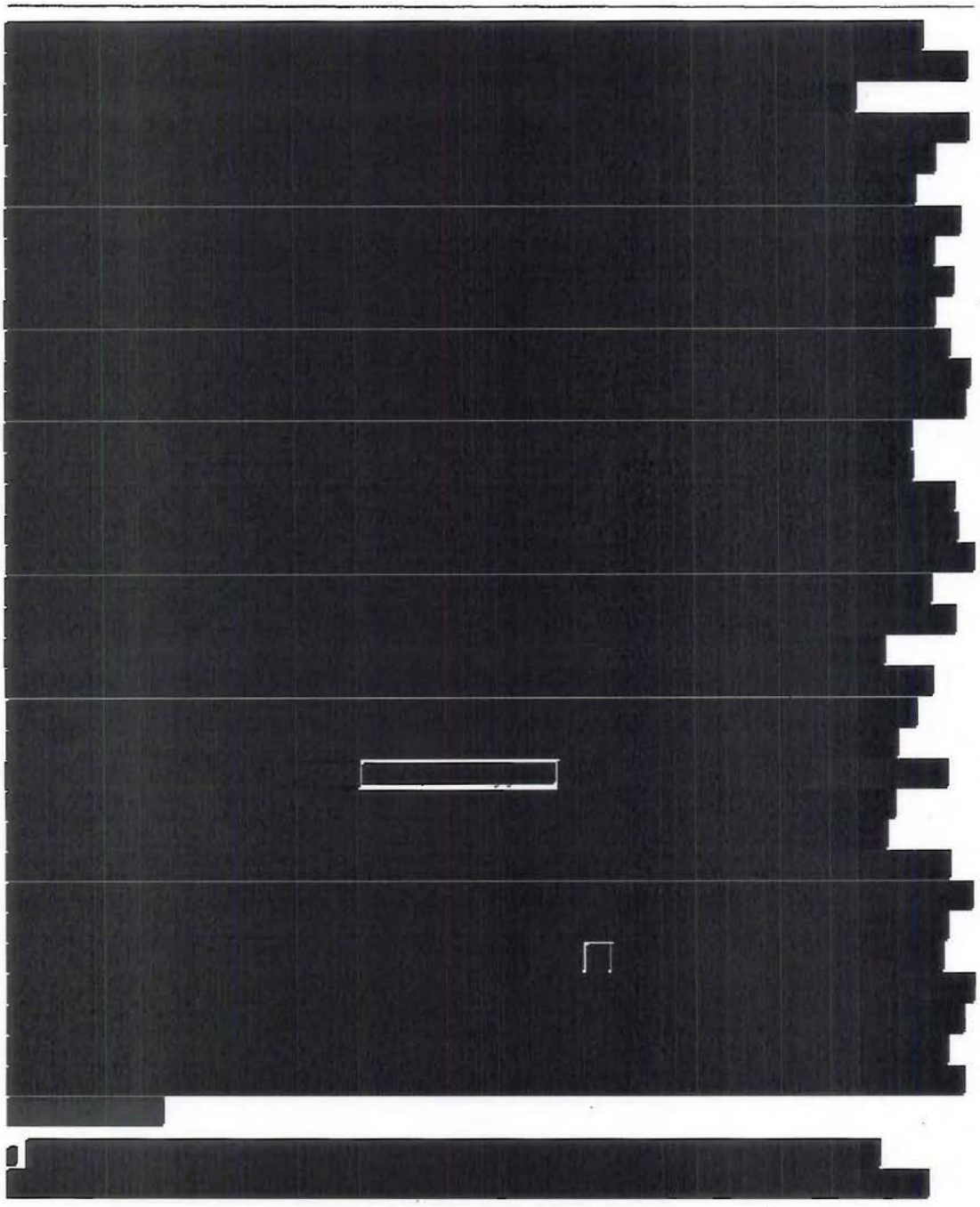
(i) Except as provided in subparagraph (ii) below, all selection terms to be used as "seeds" with which to query the BR metadata shall be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. Such approval shall be given only after the designated approving official has determined that based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [redacted]

[redacted]

[6] This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[redacted]

[redacted] provided, however, that NSA's Office of General Counsel (OGC)



~~TOP SECRET//SI//NOFORN~~

shall first determine that any selection term reasonably believed to be used by a United States (U.S.) person is not regarded as associated with [redacted] on the basis of activities that are protected by the First Amendment to the Constitution.

(ii) Selection terms that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by [redacted] including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official. The preceding sentence shall not apply to selection terms under surveillance

[redacted]

~~TOP SECRET//SI//NOFORN~~

pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that a selection term is associated with [redacted] shall be effective for: one hundred eighty days for any selection term reasonably believed to be used by a U.S. person; and one year for all other selection terms.[9,10]

---

[9] The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, articulable suspicion standard is met, but the time frame for which the selection term is or was associated with a Foreign Power shall be specified. The automated query process described in the [redacted] Declaration limits the first hop query results to the specified time frame. Analysts conducting manual queries using that selection term shall continue to properly minimize information that may be returned within query results that fall outside of that timeframe.

[redacted]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(iv) Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below.[11] This automated query process queries the collected BR metadata (in a "collection store") with RAS-approved selection terms and returns the hop-limited results from those queries to a "corporate store." The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms. The specifics of the automated query process, as described in the [redacted] Declaration, are as follows:

[redacted]

[11] This automated query process was initially approved by this Court in its [redacted] 2012 Order amending docket number [redacted]

[12] As an added protection in case technical issues prevent the process from verifying that the most up-to-date list of RAS-approved selection terms is being used, this step of the automated process checks the expiration dates of RAS-approved selection terms to confirm that the approvals for those terms have not expired. This step does not use expired RAS-approved selection terms to create the list of "authorized query terms" (described below) regardless of whether the list of RAS-approved selection terms is up-to-date.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

[redacted]

D. Results of any intelligence analysis queries of the BR metadata may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first

[redacted]

receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.[15] NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) issued on January 25, 2011, to any results from queries of the BR metadata, in any form, before the information is disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, or one of the officials listed in Section 7.3(c) of USSID 18 (i.e., the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operations Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.[16] Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch

---

[15] In addition, the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata.

[16] In the event the Government encounters circumstances that it believes necessitate the alteration of these dissemination procedures, it may obtain prospectively-applicable modifications to the procedures upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the size and nature of this bulk collection.

personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions.

E. BR metadata shall be destroyed no later than five years (60 months) after its initial collection.

F. NSA and the National Security Division of the Department of Justice (NSD/DoJ) shall conduct oversight of NSA's activities under this authority as outlined below.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.[17] OGC shall provide NSD/DoJ with copies

[17] The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his access to the BR metadata or the results from any queries of the metadata.

~~TOP SECRET//SI//NOFORN~~

of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ shall meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ shall review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.

(vii) Prior to implementation, all proposed automated query processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

G. Approximately every thirty days, NSA shall file with the Court a report that includes a discussion of NSA's application of the RAS standard, as well as NSA's implementation of the automated query process. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata.

Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand

~~TOP SECRET//SI//NOFORN~~

counterterrorism information or to assess its importance.

This authorization regarding [redacted] expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

Signed 04-25-2013 P02:26 Eastern Time
Date Time

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

Exhibit B

~~TOP SECRET//SI//NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR

13-80

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

~~TOP SECRET//SI//NOFORN~~

on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. This Order does not require Verizon to produce telephony metadata for communications wholly originating and terminating in foreign countries. Telephony metadata includes 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. Telephony metadata does not include the substantive 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.

IT IS FURTHER ORDERED that no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. A person to whom disclosure is made pursuant to (a), (b), or (c)

~~TOP SECRET//SI//NOFORN~~

shall be subject to the nondisclosure requirements applicable to a person to whom an Order is directed in the same manner as such person. Anyone who discloses to a person described in (a), (b), or (c) that the FBI or NSA has sought or obtained tangible things pursuant to this Order shall notify such person of the nondisclosure requirements of this Order. At the request of the Director of the FBI or the designee of the Director, any person making or intending to make a disclosure under (a) or (c) above shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

IT IS FURTHER ORDERED that service of this Order shall be by a method agreed upon by the Custodian of Records of Verizon and the FBI, and if no agreement is reached, service shall be personal.

-- Remainder of page intentionally left blank. --

~~TOP SECRET//SI//NOFORN~~

This authorization **requiring the production of certain call detail records or "telephony metadata" created by Verizon** expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

Signed 04-25-2013 P02:26 Eastern Time
Date Time

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

I, Beverly C. Queen, Chief Deputy Clerk, FISC, certify that this document is a true and correct copy of the original.

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 ROBERT S. MUELLER III, in his official capacity as Director of the Federal Bureau of Investigation, Defendants.	**SUPPLEMENTAL DECLARATION OF PROFESSOR EDWARD W. FELTEN** Case No. 13-cv-03994 (WHP) **ECF CASE**

SUPPLEMENTAL DECLARATION OF PROFESSOR EDWARD W. FELTEN

I, Edward W. Felten, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. Counsel for Plaintiffs in this lawsuit have asked me to submit a supplemental declaration explaining my views regarding four technological claims made by the government in its opposition to Plaintiffs' motion for a preliminary injunction:

   a. that the government does not obtain subscriber names under the mass call-tracking program, *see, e.g.*, Gov't PI Opp. 12;

   b. that so-called "three-hop analysis" of a suspect's phone number "cannot be as effectively performed" without first building a database of everyone's call records, *see, e.g.*, Gov't PI Opp. 4;

c. that telephony metadata is unique in its "standardized and inter-connected" nature, *see, e.g.*, Gov't PI Opp. 21; and

d. that it would take the government "approximately six months" to develop a method of quarantining Plaintiffs' call records if a preliminary injunction were granted, *see* Gov't PI Opp. 40.

2. Below, I address those four claims.

It is easy to correlate telephone numbers with subscriber names.

3. The government repeatedly emphasizes in its motion that, under the mass call-tracking program, it does not obtain the subscriber names associated with Americans' telephone numbers. This may be true, but it is of little significance. As I explained in my first declaration, Felten Decl. ¶ 19 & n.14, it would be trivial for the government to obtain a subscriber's name once it has that subscriber's phone number. This is so because phone numbers are unique identifiers. Like social security numbers or individual taxpayer identification numbers, phone numbers are unique to their owners.

4. It is extraordinarily easy to correlate a phone number with its unique owner. Many phone numbers are *publicly* correlated with their owners and can therefore be associated with specific persons by consulting entirely public sources. For example, many free or low-cost Internet services allow users to perform "reverse-lookup searches" to determine the owner of a particular phone number. *See, e.g.*, http://www.whitepages.com; http://www.peoplefinders.com/reverse-phone-directory. Of course, physical phone directories remain in wide circulation and have been digitized to facilitate reverse-lookup searches.

5. The government also has an array of legal authorities at its disposal to discover the subscriber names of particular phone numbers, even if those correlations are not otherwise publicly available. For example, the government may issue demands to communication service

providers for subscriber information—including subscriber names and addresses—relevant to terrorism investigations. *See* Felten Decl. ¶ 19 n.14.

Three-hop analysis can be performed without a database of all call records.

6. The government states that it could not perform three-hop analysis on a suspect's phone number without first building a database of *everyone's* call records. *See* Gov't PI Opp. 4. This is technologically incorrect. There are a number of ways in which the government could perform three-hop analysis without first building its own database of every American's call records.

7. For example, the government could obtain a single court order directing all (or perhaps even just the major) telephone companies to provide to the government the call records of everyone within three hops of a suspect's phone number. Using a straightforward algorithm (which I could describe at greater length if necessary), this order could be implemented using at most two queries to each telephone provider. Moreover, this process could easily be automated to make it virtually instantaneous. Each of the major telephone companies now subject to an order similar to the one revealed in June could create a simple electronic interface—known in the computer-programming profession as an Application Programming Interface, or API—that would be invoked by a government computer system to automate the collection of the data needed for a three-hop analysis of a specific target's phone number. The interfaces, working together to implement the algorithm referred to above, could perform the government's three-hop analysis essentially instantaneously—in a matter of seconds or less. At least one of the major telecommunications companies has already built part of such a system, providing the government with a "community of interest" search capability, which is a form of the social-graph analysis used in the mass call-tracking program. *See* Dep't of Justice, Office of the Inspector

Gen., *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* 56–64 (2010), http://www.justice.gov/oig/special/s1001r.pdf; Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. Times, Sept. 9, 2007, http://nyti.ms/g34M.

8. I have reviewed the declarations submitted by Teresa Shea and Robert Holley in support of the government's claim that the collection of all Americans' call records is necessary. Nothing in their explanation of the supposed necessity of the program alters my conclusion that three-hop analysis could be performed quickly and efficiently *without* first creating a database of the scope maintained by the government. For example, Ms. Shea suggests that the mass call-tracking program would have allowed the government to learn that a 9/11 hijacker (Khalid al-Mihdhar) was in the United States when he communicated with an al Qaeda safe house in Yemen. Shea Decl. ¶ 11. There is absolutely no need for a database of every American's call records to perform this sort of one-hop analysis. In al-Mihdar's case, the government could easily have obtained from the telephone companies (using any number of legal authorities) the call records of any American in communication with the al Qaeda safehouse. The same is true of the example provided by Mr. Holley of Najibullah Zazi. *See* Holley Decl. ¶ 26. Mr. Holley states that the NSA received Zazi's telephone number from the FBI and discovered that he was in contact with Adis Medunjanin. Again, this simple connection could have been discovered directly from the telephone companies without the need for a government database of all call records. As I explained above, though, even if these cases involved more complex connections with two or three degrees of separation, there still would be no need for the mass call-tracking program to allow the government to discover the connections.

Telephony metadata is not unique.

9. The government argues that telephony metadata is unique in that it is "standardized and inter-connected," and that these characteristics are "not common to most other types of records." Gov't PI Opp. 21. This suggestion is misleading.

10. As I explained in my first declaration, Felten Decl. ¶ 20, telephony metadata is easy to analyze because it is "structured," or highly ordered. This fact is not unique, however, to telephony metadata. Many other types of data are also structured and are therefore also easy to analyze in the aggregate.

11. Virtually every type of digital communications metadata is structured. This includes, but is by no means limited to, email metadata, Internet-usage history, and Internet chat records. Many other types of records are also structured, including financial records, credit-card records, and even portions of medical records. This is no coincidence: industry experts often develop and agree upon a standardized form for the structure of metadata or transactional data.

12. Most of these sorts of structured records are interconnected. Communications metadata are interconnected in a fairly obvious manner. But the same is true of financial and medical records. For example, prescription records memorialize the identity of the doctor, the identity of the patient, and the medicine prescribed. In a Medicare-fraud investigation, it would be possible to use prescription records to conduct a social-graph analysis, *see* Felten Decl. ¶ 48 (explaining social graphs), of a particular doctor's prescriptions. The analysis might reveal connections between several doctors' prescription habits, their overlapping patients, their connections to other doctors known to engage in fraudulent practices, or divergences between their prescription habits and the prescription habits of other doctors. *See, e.g.*, The Rise of Organized Crime in Health Care: Social Network Analytics Uncover Hidden and Complex Fraud

Schemes, *available at* http://www.writersstudio.com/samples/whitepapers/Lexis%20Nexis%20social%20network%20analytics.pdf.

13. The same sort of social-graph analysis could be applied to financial or credit-card records to uncover organized crime or fraud, because those records are also interconnected. A money-laundering investigation, for instance, could benefit from the ability to trace funds transferred from their source through a series of sham transactions and ultimately back to the original account or owner, in order to make those funds appear "clean."

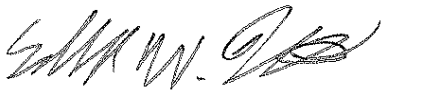
It would be feasible to quarantine the ACLU's call records.

14. The government states that it would take "approximately six months," Gov't PI Opp. 40, to devise a way in which to quarantine the ACLU's call records if the ACLU's request for a preliminary injunction were granted. This is an implausible estimate for the time necessary to develop the software to quarantine the ACLU's call records.

15. There are a number of ways that the government could efficiently and effectively quarantine the ACLU's call records. For example, the NSA could deploy an automated script that would search its database for the ACLU's call records and move those records to another database that would not be accessed except at the direction of the Court. It could also apply a filter to its three-hop analysis such that any call to or from an ACLU number would be ignored (as would any other call down the chain from any such call). Indeed, it appears that the NSA already has the ability to filter its three-hop analysis to exclude certain phone numbers. *See, e.g.*, David S. Kris, *On the Bulk Collection of Tangible Things*, 1:4 Lawfare Res. Pap. Ser. 1, 13–14 (Sept. 29, 2013) ("NSA technicians may access the metadata to make the data more useable—e.g., to create a 'defeat list' to block contact chaining through 'high volume identifiers'

presumably associated with telemarketing or similar activity." (quoting orders of the Foreign Intelligence Surveillance Court)).

16. Both of these solutions are relatively simple from a technological perspective, and it is difficult to understand how either could take significant resources to implement, much less the six months estimated by the government.



Edward W. Felten

Dated: October 25, 2013

~~TOP SECRET//SI//NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

[redacted] Docket Number: BR 13-158

MEMORANDUM

The Court has today issued the Primary Order appended hereto granting the "Application for Certain Tangible Things for Investigations to Protect Against International Terrorism" ("Application"), which was submitted to the Court on October

10, 2013, by the Federal Bureau of Investigation ("FBI"). The Application requested the issuance of orders pursuant to 50 U.S.C. § 1861, as amended (also known as Section 215 of the USA PATRIOT Act), requiring the ongoing daily production to the National Security Agency ("NSA") of certain telephone call detail records in bulk.

The Primary Order appended hereto renews the production of records made pursuant to the similar Primary Order issued by the Honorable Claire V. Eagan of this Court on July 19, 2013 in Docket Number BR 13-109 ("July 19 Primary Order"). On August 29, 2013, Judge Eagan issued an Amended Memorandum Opinion setting forth her reasons for issuing the July 19 Primary Order ("August 29 Opinion"). Following a declassification review by the Executive Branch, the Court published the July 19 Primary Order and August 29 Opinion in redacted form on September 17, 2013.

The call detail records to be produced pursuant to the orders issued today in the above-captioned docket are identical in scope and nature to the records produced in response to the orders issued by Judge Eagan in Docket Number BR 13-109. The records will be produced on terms identical to those set out in Judge Eagan's July 19 Primary Order and for the same purpose, and the information acquired by NSA through the production will be subject to the same provisions for oversight and identical restrictions on access, retention, and dissemination.

~~TOP SECRET//SI//NOFORN~~

This is the first time that the undersigned has entertained an application requesting the bulk production of call detail records. The Court has conducted an independent review of the issues presented by the application and agrees with and adopts Judge Eagan's analysis as the basis for granting the Application. The Court writes separately to discuss briefly the issues of "relevance" and the inapplicability of the Fourth Amendment to the production.

Although the definition of relevance set forth in Judge Eagan's decision is broad, the Court is persuaded that that definition is supported by the statutory analysis set out in the August 29 Opinion. That analysis is reinforced by Congress's re-enactment of Section 215 after receiving information about the government's and the FISA Court's interpretation of the statute. Although the existence of this program was classified until several months ago, the record is clear that before the 2011 re-enactment of Section 215, many Members of Congress were aware of, and each Member had the opportunity to learn about, the scope of the metadata collection and this Court's interpretation of Section 215. Accordingly, the re-enactment of Section 215 without change in 2011 triggered the doctrine of ratification through re-enactment, which provides a strong reason for this Court to continue to adhere to its prior interpretation of Section 215. See Lorillard v. Pons, 434 U.S. 575, 580 (1978); see also EEOC v. Shell Oil Co., 466 U.S. 54, 69 (1984); Haig v. Agee, 453 U.S. 280, 297-98 (1981).

The undersigned also agrees with Judge Eagan that, under Smith v. Maryland, 442 U.S. 735 (1979), the production of call detail records in this matter does not constitute a search under the Fourth Amendment. In Smith, the Supreme Court held that the use of a pen register to record the numbers dialed from the defendant's home telephone did not constitute a search for purposes of the Fourth Amendment. In so holding, the Court stressed that the information acquired did not include the contents of any communication and that the information was acquired by the government from the telephone company, to which the defendant had voluntarily disclosed it for the purpose of completing his calls.

The Supreme Court's more recent decision in United States v. Jones, — U.S. —, 132 S. Ct. 945 (2012), does not point to a different result here. Jones involved the acquisition of a different type of information through different means. There, law enforcement officers surreptitiously attached a Global Positioning System (GPS) device to the defendant's vehicle and used it to track his location for 28 days. The Court held in Justice Scalia's majority opinion that the officers' conduct constituted a search under the Fourth Amendment because the information at issue was obtained by means of a physical intrusion on the defendant's vehicle, a constitutionally-protected area. The majority declined to decide whether use of the GPS device, without the physical intrusion, impinged upon a reasonable expectation of privacy.

Five Justices in Jones signed or joined concurring opinions suggesting that the precise, pervasive monitoring by the government of a person's location could trigger Fourth Amendment protection even without any physical intrusion. This matter, however, involves no such monitoring. Like Smith, this case concerns the acquisition of non-content metadata other than location information. See Aug. 29 Op. at 29 at 4 n.5; id. at 6 & n.10.

Justice Sotomayor stated in her concurring opinion in Jones that it "may be necessary" for the Supreme Court to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," which she described as "ill suited to the digital age." See Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citing Smith and United States v. Miller, 425 U.S. 435, 443 (1976), as examples of decisions relying upon that premise). But Justice Sotomayor also made clear that the Court undertook no such reconsideration in Jones. See id. ("Resolution of these difficult questions in this case is unnecessary, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision."). The Supreme Court may some day revisit the third-party disclosure principle in the context of twenty-first century communications technology, but that day has not arrived. Accordingly, Smith remains controlling with respect to the acquisition by the government from service providers of non-content telephony

metadata such as the information to be produced in this matter.

In light of the public interest in this matter and the government's declassification of related materials, including substantial portions of Judge Eagan's August 29 Opinion and July 19 Primary Order, the undersigned requests pursuant to FISC Rule 62 that this Memorandum and the accompanying Primary Order also be published and directs such request to the Presiding Judge as required by the Rule.

ENTERED this 11th day of October, 2013.

Mary A. McLaughlin

MARY A. McLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court

[redacted]

~~TOP SECRET//SI//NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket Number: BR 13-158

PRIMARY ORDER

A verified application having been made by the Director of the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, requiring the

~~TOP SECRET//SI//NOFORN~~

Derived from: Pleadings in the above-captioned docket
Declassify on: [redacted]

~~TOP SECRET//SI//NOFORN~~

production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:

1. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things. [50 U.S.C. § 1861(c)(2)(D)]

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number BR 13-109 and its predecessors. [50 U.S.C. § 1861(c)(1)]

~~TOP SECRET//SI//NOFORN~~

Accordingly, and as further explained in the accompanying Memorandum, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application is GRANTED, and it is

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata"[1] created by [redacted]

B. The Custodian of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis

[1] For purposes of this Order "telephony metadata" includes 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. Telephony metadata does not include the substantive 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. Furthermore, this Order does not authorize the production of cell site location information (CSLI).

thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by [redacted] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [redacted]

(2) With respect to any information the FBI receives as a result of this Order (information that is disseminated to it by NSA), the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General's Guidelines for Domestic FBI Operations* (September 29, 2008).

(3) With respect to the information that NSA receives as a result of this Order, NSA shall strictly adhere to the following minimization procedures:

A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors ("BR metadata") for any purpose except as described herein.

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA's control.[2] The BR metadata shall carry unique markings such

[2] The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA shall ensure that any access

~~TOP SECRET//SI//NOFORN~~

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.[3] Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms[4] that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes,

---

or use of the BR metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

[3] The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA, will not receive special training regarding the authority granted herein.

[redacted]

~~TOP SECRET//SI//NOFORN~~

but the results of any such queries will not be used for intelligence analysis purposes. An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

C. NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through queries of the BR metadata to obtain contact chaining information as described in paragraph 17 of the Declaration o[redacted] attached to the application as Exhibit A, using selection terms approved as "seeds" pursuant to the RAS approval process described below.[5] NSA shall ensure,

[5] For purposes of this Order, "National Security Agency" and "NSA personnel" are defined as any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to FISA if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). NSA personnel shall not disseminate BR metadata outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of this Order that are applicable to the NSA.

~~TOP SECRET//SI//NOFORN~~

through adequate and appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.[6]

(i) Except as provided in subparagraph (ii) below, all selection terms to be used as "seeds" with which to query the BR metadata shall be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. Such approval shall be given only after the designated approving official has determined that based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [redacted]

[redacted]

[6] This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[redacted]

~~TOP SECRET//SI//NOFORN~~

[redacted] provided, however, that NSA's Office of General Counsel (OGC)

[redacted]

shall first determine that any selection term reasonably believed to be used by a United States (U.S.) person is not regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution.

(ii) Selection terms that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by [redacted] including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official. The preceding sentence shall not apply to selection terms under surveillance

[redacted]

~~TOP SECRET//SI//NOFORN~~

pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that a selection term is associated with [redacted] shall be effective for: one hundred eighty days for any selection term reasonably believed to be used by a U.S. person; and one year for all other selection terms.[9,10]

---

[9] The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, articulable suspicion standard is met, but the time frame for which the selection term is or was associated with a Foreign Power shall be specified. The automated query process described in the [redacted] Declaration limits the first hop query results to the specified time frame. Analysts conducting manual queries using that selection term shall continue to properly minimize information that may be returned within query results that fall outside of that timeframe.

[10] The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders. NSA shall store, handle, and disseminate call detail records produced in response to this Court's Orders pursuant to this Orde[redacted]

~~TOP SECRET//SI//NOFORN~~

(iv) Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below.[11] This automated query process queries the collected BR metadata (in a "collection store") with RAS-approved selection terms and returns the hop-limited results from those queries to a "corporate store." The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms. The specifics of the automated query process, as described in the [redacted] Declaration, are as follows:

[redacted]

[11] This automated query process was initially approved by this Court in its November 8, 2012 Order amending docket number BR 12-178.

[12] As an added protection in case technical issues prevent the process from verifying that the most up-to-date list of RAS-approved selection terms is being used, this step of the automated process checks the expiration dates of RAS-approved selection terms to confirm that the approvals for those terms have not expired. This step does not use expired RAS-approved selection terms to create the list of "authorized query terms" (described below) regardless of whether the list of RAS-approved selection terms is up-to-date.

~~TOP SECRET//SI//NOFORN~~

[redacted]

D. Results of any intelligence analysis queries of the BR metadata may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first

[redacted]

receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.[15] NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) issued on January 25, 2011, to any results from queries of the BR metadata, in any form, before the information is disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, or one of the officials listed in Section 7.3(c) of USSID 18 (i.e., the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operations Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.[16] Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch

[15] In addition, the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata.

[16] In the event the Government encounters circumstances that it believes necessitate the alteration of these dissemination procedures, it may obtain prospectively-applicable modifications to the procedures upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the size and nature of this bulk collection.

personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions.

E. BR metadata shall be destroyed no later than five years (60 months) after its initial collection.

F. NSA and the National Security Division of the Department of Justice (NSD/DoJ) shall conduct oversight of NSA's activities under this authority as outlined below.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.[17] OGC shall provide NSD/DoJ with copies

[17] The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his access to the BR metadata or the results from any queries of the metadata.

of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ shall meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

~~TOP SECRET//SI//NOFORN~~

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ shall review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.

(vii) Other than the automated query process described in the [redacted] Declaration and this Order, prior to implementation of any new or modified automated query processes, such new or modified processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

G. Approximately every thirty days, NSA shall file with the Court a report that includes a discussion of NSA's application of the RAS standard, as well as NSA's implementation and operation of the automated query process. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata.

Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials

~~TOP SECRET//SI//NOFORN~~

authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.

This authorization regarding [redacted] expires on the 3RD day of January, 2014, at 5:00 p.m., Eastern Time.

Signed 10-11-2013 P12:05 Eastern Time
Date Time

Mary A. McLaughlin
MARY A. MCLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

[redacted] : Docket No.: BR 08-13

SUPPLEMENTAL OPINION

This Supplemental Opinion memorializes the Court's reasons for concluding that the records to be produced pursuant to the orders issued in the above-referenced docket number are properly subject to production pursuant to 50 U.S.C.A. § 1861 (West 2003 & Supp. 2008), notwithstanding the provisions of 18 U.S.C.A. §§ 2702-2703 (West 2000 & Supp. 2008), amended by Public Law 110-401, § 501(b)(2) (2008).

As requested in the application, the Court is ordering production of telephone "call detail records or 'telephony metadata,'" which "includes comprehensive communications routing information, including but not limited to session identifying information . . ., trunk identifier, telephone calling card numbers, and time and duration of [the] calls," but "does not include the substantive content of any communication." Application at 9; Primary Order at 2. Similar productions have been ordered by judges of the Foreign Intelligence Surveillance Court ("FISC"). See Application at 17. However, this is the first application in which the government has identified the provisions of 18 U.S.C.A. §§ 2702-2703 as potentially relevant to whether such orders could properly be issued under 50 U.S.C.A. § 1861. See Application at 6-8.

Pursuant to section 1861, the government may apply to the FISC "for an order requiring the production of any tangible things (including books, records, papers, documents, and other items)." 50 U.S.C.A. § 1861(a)(1) (emphasis added). The FISC is authorized to issue the order, "as requested, or as modified," upon a finding that the application meets the requirements of that section. Id. at § 1861(c)(1). Under the rules of statutory construction, the use of the word "any" in a statute naturally connotes "an expansive meaning," extending to all members of a common set, unless Congress employed "language limiting [its] breadth." United States v. Gonzales, 520 U.S. 1, 5 (1997); accord Ali v. Federal Bureau of Prisons, 128 S. Ct. 831, 836 (2008)

("Congress' use of 'any' to modify 'other law enforcement officer' is most naturally read to mean law enforcement officers of whatever kind.").[1]

However, section 2702, by its terms, describes an apparently exhaustive set of circumstances under which a telephone service provider may provide to the government non-content records pertaining to a customer or subscriber. See § 2702(a)(3) (except as provided in § 2702(c), a provider "shall not knowingly divulge a record or other [non-content] information pertaining to a subscriber or customer . . . to any governmental entity"). In complementary fashion, section 2703 describes an apparently exhaustive set of means by which the government may compel a provider to produce such records. See § 2703(c)(1) ("A governmental entity may require a provider . . . to disclose a record or other [non-content] information pertaining to a subscriber . . . or customer . . . only when the governmental entity" proceeds in one of the ways described in § 2703(c)(1)(A)-(E)) (emphasis added). Production of records pursuant to a FISC order under section 1861 is not expressly contemplated by either section 2702(c) or section 2703(c)(1)(A)-(E).

If the above-described statutory provisions are to be reconciled, they cannot all be given their full, literal effect. If section 1861 can be used to compel production of call detail records, then the prohibitions of section 2702 and 2703 must be understood to have an implicit exception for production in response to a section 1861 order. On the other hand, if sections 2702 and 2703 are understood to prohibit the use of section 1861 to compel production of call detail records, then the expansive description of tangible things obtainable under section 1861(a)(1) must be construed to exclude such records.

The apparent tension between these provisions stems from amendments enacted by Congress in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act"), Public Law 107-56, October 26, 2001, 115 Stat. 272. Prior to the USA PATRIOT Act, only limited types of records, not

---

[1] The only express limitation on the type of tangible thing that can be subject to a section 1861 order is that the tangible thing "can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." Id. at § 1861(c)(2)(D). Call detail records satisfy this requirement, since they may be obtained by (among other means) a "court order for disclosure" under 18 U.S.C.A. § 2703(d). Section 2703(d) permits the government to obtain a court order for release of non-content records, or even in some cases of the contents of a communication, upon a demonstration of relevance to a criminal investigation.

including call detail records, were subject to production pursuant to FISC orders.[2] Section 215 of the USA PATRIOT Act replaced this prior language with the broad description of "any tangible thing" now codified at section 1861(a)(1). At the same time, the USA PATRIOT Act amended sections 2702 and 2703 in ways that seemingly re-affirmed that communications service providers could divulge records to the government only in specified circumstances,[3] without expressly referencing FISC orders issued under section 1861.

The government argues that section 1861(a)(3) supports its contention that section 1861(a)(1) encompasses the records sought in this case. Under section 1861(a)(3), which Congress enacted in 2006,[4] applications to the FISC for production of several categories of sensitive records, including "tax return records" and "educational records," may be made only by the Director, the Deputy Director or the Executive Assistant Director for National Security of the Federal Bureau of Investigation ("FBI"). 18 U.S.C.A. § 1861(a)(3). The disclosure of tax return records[5] and educational records[6] is specifically regulated by other federal statutes, which do not by their own terms contemplate production pursuant to a section 1861 order. Nonetheless, Congress clearly intended that such records could be obtained under a section 1861 order, as demonstrated by their inclusion in section 1861(a)(3). But, since the records of telephone service providers are not mentioned in section 1861(a)(3), this line of reasoning is not directly on point. However, it does at least demonstrate that Congress may have intended the sweeping description of tangible items obtainable under section 1861 to encompass the records of telephone service providers, even though the specific provisions of sections 2702 and 2703 were not amended in order to make that intent unmistakably clear.

---

[2] See 50 U.S.C.A. § 1862(a) (West 2000) (applying to records of transportation carriers, storage facilities, vehicle rental facilities, and public accommodation facilities).

[3] Specifically, the USA PATRIOT Act inserted the prohibition on disclosure to governmental entities now codified at 18 U.S.C.A. § 2702(a)(3), and exceptions to this prohibition now codified at 18 U.S.C.A. § 2702(c). See USA PATRIOT Act § 212(a)(1)(B)(iii) & (E). The USA PATRIOT Act also amended the text of 18 U.S.C.A. § 2703(c)(1) to state that the government may require the disclosure of such records only in circumstances specified therein. See USA PATRIOT Act § 212(b)(1)(C)(i).

[4] See Public Law 109-177 § 106(a)(2) (2006).

[5] See 26 U.S.C.A. § 6103(a) (West Supp. 2008), amended by Public Law 110-328 § 3(b)(1) (2008).

[6] See 20 U.S.C.A. § 1232g(b) (West 2000 & Supp. 2008).

The Court finds more instructive a separate provision of the USA PATRIOT Act, which also pertains to governmental access to non-content records from communications service providers. Section 505(a) of the USA PATRIOT Act amended provisions, codified at 18 U.S.C.A. § 2709 (West 2000 & Supp. 2008), enabling the FBI, without prior judicial review, to compel a telephone service provider to produce "subscriber information and toll billing records information." 18 U.S.C.A. § 2709(a).[7] Most pertinently, section 505(a)(3)(B) of the USA PATRIOT Act lowered the predicate required for obtaining such information to a certification submitted by designated FBI officials asserting its relevance to an authorized foreign intelligence investigation.[8]

Indisputably, section 2709 provides a means for the government to obtain non-content information in a manner consistent with the text of sections 2702-2703.[9] Yet section 2709 merely requires an FBI official to provide a certification of relevance. In comparison, section 1861 requires the government to provide to the FISC a "statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant" to a foreign intelligence investigation,[10] and the FISC to determine that the application satisfies this

---

[7] This process involves service of a type of administrative subpoena, commonly known as a "national security letter." David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 19:2 (2007).

[8] Specifically, a designated FBI official must certify that the information or records sought are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States." 18 U.S.C.A. § 2709(b)(1)-(2) (West Supp. 2008). Prior to the USA PATRIOT Act, the required predicate for obtaining "local and long distance toll billing records of a person or entity" was "specific and articulable facts giving reason to believe that the person or entity . . . is a foreign power or an agent of a foreign power." See 18 U.S.C.A. § 2709(b)(1)(B) (West 2000).

[9] Section 2703(c)(2) permits the government to use "an administrative subpoena" to obtain certain categories of non-content information from a provider, and section 2709 concerns use of an administrative subpoena. See note 7 supra.

[10] 50 U.S.C.A. § 1861(b)(2)(A). More precisely, the investigation must be "an authorized investigation (other than a threat assessment) . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities," id., "provided that such investigation of a United States

(continued...)

requirement, see 50 U.S.C.A. § 1861(c)(1), before records are ordered produced. It would have been anomalous for Congress, in enacting the USA PATRIOT Act, to have deemed the FBI's application of a "relevance" standard, without prior judicial review, sufficient to obtain records subject to sections 2702-2703, but to have deemed the FISC's application of a closely similar "relevance" standard insufficient for the same purpose. This anomaly is avoided by interpreting sections 2702-2703 as implicitly permitting the production of records pursuant to a FISC order issued under section 1861.

It is the Court's responsibility to attempt to interpret a statute "as a symmetrical and coherent regulatory scheme, and fit, if possible, all parts into an harmonious whole." Food & Drug Admin. v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000) (internal quotations and citations omitted). For the foregoing reasons, the Court is persuaded that this objective is better served by the interpretation that the records sought in this case are obtainable pursuant to a section 1861 order.

However, to the extent that any ambiguity may remain, it should be noted that the legislative history of the USA PATRIOT Act is consistent with this expansive interpretation of section 1861(a)(1). See 147 Cong. Rec. 20,703 (2001) (statement of Sen. Feingold) (section 215 of USA PATRIOT Act "permits the Government . . . to compel the production of records from any business regarding any person if that information is sought in connection with an investigation of terrorism or espionage;" "all business records can be compelled, including those containing sensitive personal information, such as medical records from hospitals or doctors, or educational records, or records of what books somebody has taken out from the library") (emphasis added). In this regard, it is significant that Senator Feingold introduced an amendment to limit the scope of section 1861 orders to records "not protected by any Federal or State law governing access to the records for intelligence or law enforcement purposes," but this limitation was not adopted. See 147 Cong. Rec. 19,530 (2001).

ENTERED this 12th day of December, 2008, regarding Docket No. BR 08-13.

REGGIE B. WALTON
Judge, United States Foreign
Intelligence Surveillance Court

---

[10](...continued)
person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." Id. § 1861(a)(1). The application must also include minimization procedures in conformance with statutory requirements, which must also be reviewed by the FISC. Id. § 1861(b)(2)(B), (c)(1), & (g).

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION, *et al.*,	:	13 Civ. 3994 (WHP)
Plaintiffs,	:	MEMORANDUM & ORDER
-against-	:	
JAMES R. CLAPPER, *et al.*	:	
Defendants.	:	

WILLIAM H. PAULEY III, District Judge:

The September 11th terrorist attacks revealed, in the starkest terms, just how dangerous and interconnected the world is. While Americans depended on technology for the conveniences of modernity, al-Qaeda plotted in a seventh-century milieu to use that technology against us. It was a bold jujitsu. And it succeeded because conventional intelligence gathering could not detect diffuse filaments connecting al-Qaeda.

Prior to the September 11th attacks, the National Security Agency ("NSA") intercepted seven calls made by hijacker Khalid al-Mihdhar, who was living in San Diego, California, to an al-Qaeda safe house in Yemen. The NSA intercepted those calls using overseas signals intelligence capabilities that could not capture al-Mihdhar's telephone number identifier. Without that identifier, NSA analysts concluded mistakenly that al-Mihdhar was overseas and not in the United States. Telephony metadata would have furnished the missing information and might have permitted the NSA to notify the Federal Bureau of Investigation ("FBI") of the fact

that al-Mihdhar was calling the Yemeni safe house from inside the United States. [1]

The Government learned from its mistake and adapted to confront a new enemy: a terror network capable of orchestrating attacks across the world. It launched a number of counter-measures, including a bulk telephony metadata collection program—a wide net that could find and isolate gossamer contacts among suspected terrorists in an ocean of seemingly disconnected data.

This blunt tool only works because it collects everything. Such a program, if unchecked, imperils the civil liberties of every citizen. Each time someone in the United States makes or receives a telephone call, the telecommunications provider makes a record of when, and to what telephone number the call was placed, and how long it lasted. The NSA collects that telephony metadata. If plumbed, such data can reveal a rich profile of every individual as well as a comprehensive record of people's associations with one another.

The natural tension between protecting the nation and preserving civil liberty is squarely presented by the Government's bulk telephony metadata collection program. Edward Snowden's unauthorized disclosure of Foreign Intelligence Surveillance Court ("FISC") orders has provoked a public debate and this litigation. While robust discussions are underway across the nation, in Congress, and at the White House, the question for this Court is whether the Government's bulk telephony metadata program is lawful. This Court finds it is. But the question of whether that program should be conducted is for the other two coordinate branches of Government to decide.

---

[1] See generally, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States [hereinafter the "9/11 Report"] (2004).

The American Civil Liberties Union, the American Civil Liberties Union Foundation, the New York Civil Liberties Union, and the New York Civil Liberties Foundation (collectively, "the ACLU" or Plaintiffs) bring this action challenging the legality of the NSA's telephony metadata collection program. James R. Clapper, the Director of National Intelligence; Keith B. Alexander, the Director of NSA and Chief of the Central Security Service; Charles T. Hagel, the Secretary of Defense; Eric H. Holder, the Attorney General of the United States; and James B. Comey, the Director of the FBI (collectively, "Defendants" or the "Government") are Executive Branch Department and Agency heads involved with the bulk telephony metadata collection program. The ACLU moves for a preliminary injunction and the Government moves to dismiss the complaint. For the reasons that follow, this Court grants the Government's motion to dismiss and denies the ACLU's motion for a preliminary injunction.

BACKGROUND

I. Foreign Intelligence Surveillance Act

In 1972, the Supreme Court recognized that "criminal surveillances and those involving domestic security" are distinct, and that "Congress may wish to consider protective standards for the latter which differ from those already prescribed for [criminal surveillances]." United States v. U.S. Dist. Court for East. Dist. of Mich. (Keith), 407 U.S. 297, 322 (1972). "Although the Keith opinion expressly disclaimed any ruling 'on the scope of the President's surveillance power with respect to the activities of foreign powers,' it implicitly suggested that a special framework for foreign intelligence surveillance might be constitutionally permissible." Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013) (quoting Keith, 407 U.S. at 322–23) (internal citations omitted).

In 1975, Congress organized the Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities, known as the "Church Committee," to investigate and report on the Government's intelligence-gathering operations. The Church Committee concluded that the Executive Branch had engaged in widespread surveillance of U.S. citizens and that Congress needed to provide clear boundaries for foreign intelligence gathering.

In 1978, Congress did just that. Legislating against the backdrop of Keith and the Church Committee findings, Congress enacted the Foreign Intelligence Surveillance Act of 1978 (FISA). Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801 to 1885c). FISA requires the Government to obtain warrants or court orders for certain foreign intelligence surveillance activities and created the FISC to review those applications and grant them if appropriate.

While the FISC is composed of Article III judges, it operates unlike any other Article III court. Proceedings in Article III courts are public. And the public enjoys a "general right to inspect and copy public records and documents, including judicial records and documents." Nixon v. Warner Comm'cns, Inc., 435 U.S. 589, 597–98 (1978) (footnotes omitted). "The presumption of access is based on the need for federal courts, although independent—indeed, particularly because they are independent—to have a measure of accountability and for the public to have confidence in the administration of justice." Lugosch v. Pyramid Co. of Onondaga, 435 F.3d 110, 119 (2d Cir. 2006) (quoting United States v. Amodeo, 71 F.3d 1044, 1048 (2d Cir. 1995)); see also Standard Chartered Bank Int'l (Americas) Ltd. v. Calvo, 757 F. Supp. 2d 258, 259–60 (S.D.N.Y. 2010).[2]

[2] The Judicial Conference of the United States reaffirmed the public interest in the efficient and

But FISC proceedings are secret. Congress created a secret court that operates in a secret environment to provide judicial oversight of secret Government activities. See 50 U.S.C. § 1803(c) ("The record of proceedings [in the FISC] shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence."). While the notion of secret proceedings may seem antithetical to democracy, the Founding Fathers recognized the need for the Government to keep secrets. See U.S. Const. Art. I § 5, cl. 3. ("Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy.")

Congress has long appreciated the Executive's paramount need to keep matters of national security secret. See, e.g., 5 U.S.C. § 552(b)(1)(A) (first enacted July 4, 1966, Pub. L. 89-487) (The Executive is not required to disclose "matters that are specifically authorized . . . by an Executive order to be kept secret in the interest of national defense" under the Freedom of Information Act). Indeed, "[s]ecrecy and dispatch" are essential ingredients to the President's effective discharge of national security. See The Federalist No. 70, at 472 (Alexander Hamilton) (J Cooke ed., 1961). FISC is an exception to the presumption of openness and transparency—in matters of national security, the Government must be able to keep its means and methods secret from its enemies.

In 1998, Congress amended FISA to allow for orders directing common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities to provide

---

transparent administration of justice by acknowledging that "sealing an entire case file is a last resort." Judicial Conference of the United States, Judicial Conference Policy on Sealed Cases (Sept. 13, 2011), available at http://www.uscourts.gov/uscourts/News/2011/docs/JudicialConferencePolicyOnSealedCivilCases2011.pdf.

business records to the Government. See Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, § 602, 112 Stat. 2396, 2410 (1998). These amendments required the Government to make a showing of "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." § 602.

After the September 11th attacks, Congress expanded the Government's authority to obtain additional records. See USA PATRIOT Act of 2001, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861) ("section 215"). Section 215 allows the Government to obtain an order "requiring the production of any tangible things (including books, records, papers, documents, and other items)," eliminating the restrictions on the types of businesses that can be served with such orders and the requirement that the target be a foreign power or their agent. The Government invoked this authority to collect virtually all call detail records or "telephony metadata." See infra, Part II. See generally David S. Kris, On the Bulk Collection of Tangible Things, 1 Lawfare Res. Pap. Ser. 4 (2013).

Bulk telephony metadata collection under FISA is subject to extensive oversight by all three branches of government. It is monitored by the Department of Justice, the Intelligence Community, the FISC, and Congress. See Administration White Paper, Bulk Collection of the Telephony Metadata Under Section 215 of the USA Patriot Act 3 (Aug. 9, 2013) [hereinafter "White Paper"]. To collect bulk telephony metadata, the Executive must first seek judicial approval from the FISC. 50 U.S.C. § 1861. Then, on a semi-annual basis, it must provide reports to the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committees on the

Judiciary of the House of Representatives and the Senate. 50 U.S.C. § 1871(a). Those reports must include: (1) a summary of significant legal interpretations of section 215 involving matters before the FISC; and (2) copies of all decisions, orders, or opinions of the FISC that include significant construction or interpretation of section 215. 50 U.S.C. § 1871(c).

Since the initiation of the program, a number of compliance and implementation issues were discovered and self-reported by the Government to the FISC and Congress.

> In accordance with the [FISA] Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The incidents, and the Court's responses, were also reported to the Intelligence Committees in great detail. The Committees, the Court, and the Executive Branch have responded actively to the incidents. The Court has imposed additional safeguards. In response to compliance problems, the Director of NSA also ordered 'end-to-end' reviews of the section 215 . . . programs, and created a new position, the Director of Compliance, to help ensure the integrity of future collection.

Report on the NSA's Bulk Collection Programs for USA PATRIOT Act Reauthorization (ECF No. 33-5) [hereinafter "NSA Report"]. The NSA addressed these problems. For example, in 2011, FISC Judge Bates engaged in a protracted iterative process with the Government—that included numerous written submissions, meetings between court staff and the Justice Department, and a hearing—over the Government's application for reauthorization of another FISA collection program. That led to a complete review of that program's collection and querying methods. See generally Mem. Op. [REDACTED], No. [REDACTED] (F.I.S.C. Oct. 3, 2011) (Bates, J.) available at http://icontherecord.tumblr.com/tagged/declassified.[3]

[3] The iterative process Judge Bates describes is routine in the FISC and demonstrates the FISC does not "rubberstamp" applications for section 215 orders.

In August 2013, FISC Judge Eagan noted, "[t]he 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 Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], Case No. BR 13-109, amended slip op. at 5 n.8 (F.I.S.C., Aug. 29, 2013) (released in redacted form Sept. 17, 2013). And Congress repeatedly reauthorized the statute.

In recognition of the broad intelligence gathering capability Congress granted to the Executive Branch, section 215 included a sunset provision terminating that authority at the

---

> When [the Government] prepares an application for [a section 215 order, it] first submit[s] to the [FISC] what's called a "read copy," which the court staff will review and comment on. [A]nd they will almost invariably come back with questions, concerns, problems that they see. And there is an iterative process back and forth between the Government and the [FISC] to take care of those concerns so that at the end of the day, we're confident that we're presenting something that the [FISC] will approve. That is hardly a rubber stamp. It's rather extensive and serious judicial oversight of this process.

Testimony before the House Permanent Select Committee on Intelligence, dated Jun. 18, 2013, Robert Litt, General Counsel, Office of the Director of National Intelligence at 17–18 (ECF No. 33-13).

end of 2005. But the war on terror did not end. Congress has renewed section 215 seven times.[4] In 2006, Congress amended section 215 to require the Government to provide "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106, 120 Stat. 192, 196 (2006) (codified as amended at 50 U.S.C. § 1861).

II. NSA Bulk Telephony Metadata Collection

On June 5, 2013, The Guardian published a then-classified FISC "Secondary Order" directing Verizon Business Network Services to provide the NSA "on an ongoing daily basis . . . all call detail records or 'telephony metadata'" for all telephone calls on its network from April 25, 2013 to July 19, 2013. See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From Verizon Bus. Network Servs., Inc. ex. rel. MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs., No. BR 13-80, slip op. at 2–4 (F.I.S.C. Apr. 25, 2013) ("Secondary Order"). "Telephony metadata" includes, as to each call, the telephone numbers that placed and received the call, the date, time, and duration of the call, other session-identifying information (for example, International Mobile Subscriber Identity number, International Mobile

[4] See An Act to Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of that Act and the Lone Wolf Provision of the Intelligence Reform and Terrorism Provision Act of 2004 to July 1, 2006, Pub. L. No. 109-160, 119 Stat. 2957 (2005); An Act to Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of Such Act, Pub. L. No. 109-170, 120 Stat. 3 (2006); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006); Department of Defense Appropriations Act, 2010, Pub. L. No. 111-118, 123 Stat. 3409 (2009); An Act to Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, Pub. L. No. 111-141, 124 Stat. 37 (2010); FISA Sunsets Extension Act of 2011, Pub. L. No. 112-3, 125 Stat. 5 (2011); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011).

station Equipment Identity number, et cetera), trunk identifier, and any telephone calling card number. See Decl. of Teresa H. Shea, Director of the Signals Intelligence Directorate, NSA, dated Oct. 1, 2013, ¶ 15 (ECF No. 63); Secondary Order at 2. It does not include the content of any call, the name, address, or financial information of parties to the call, or any cell site location information. See Shea Decl. ¶ 15; Secondary Order at 2. In response to the unauthorized disclosure of the Secondary Order, the Government acknowledged that since May 2006, it has collected this information for substantially every telephone call in the United States, including calls between the United States and a foreign country and calls entirely within the United States. See Shea Decl. ¶ 13; White Paper at 3.

The Secondary Order was issued pursuant to a "Primary Order" setting out certain "minimization" requirements for the use of telephony metadata. See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From [REDACTED], No. BR 13-80 (F.I.S.C. Apr. 25, 2013) ("Primary Order"). The NSA stores the metadata in secure networks and access is limited to authorized personnel. Primary Order at 4–5. Though metadata for all telephone calls is collected, there are restrictions on how and when it may be accessed and reviewed. The NSA may access the metadata to further a terrorism investigation only by "querying" the database with a telephone number, or "identifier," that is associated with a foreign terrorist organization. Shea Decl. ¶ 19; Primary Order at 6–9. Before the database may be queried, a high-ranking NSA official or one of twenty specially-authorized officials must determine there is "reasonable articulable suspicion" that the identifier is associated with an international terrorist organization that is the subject of an FBI investigation. Shea Decl. ¶¶ 20, 31; Primary Order at 7. The "reasonable articulable suspicion" requirement ensures an "ordered

and controlled" query and prevents general data browsing. Shea Decl. ¶ 20. An identifier reasonably believed to be used by a U.S. person may not be regarded as associated with a terrorist organization solely on the basis of activities protected by the First Amendment. Shea Decl. ¶¶ 20, 31; Primary Order at 9. An identifier used to query telephony metadata is referred to as a "seed." Shea Decl. ¶ 20.

The results of a query include telephone numbers that have been in contact with the seed, as well as the dates, times, and durations of those calls, but not the identities of the individuals or organizations associated with responsive telephone numbers. Shea Decl. ¶ 21. The query results also include second and third-tier contacts of the seed, referred to as "hops." Shea Decl. ¶ 22. The first "hop" captures telephony metadata for the set of telephone numbers in direct contact with the seed. The second "hop" reaches telephony metadata for the set of telephone numbers in direct contact with any first "hop" telephone number. The third "hop" corrals telephony metadata for the set of telephone numbers in direct contact with any second "hop" telephone number. Shea Decl. ¶ 22. The NSA takes this information and determines "which of the results are likely to contain foreign intelligence information, related to counterterrorism, that would be of investigative value to FBI (or other intelligence agencies)." Shea Decl. ¶ 26. They provide only this digest to the FBI. Moreover, metadata containing information concerning a U.S. person may only be shared outside the NSA if an official determines "that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance." Primary Order at 16–17; see also Shea Decl. ¶¶ 28, 32.

Through this sifting, "only a very small percentage of the total data collected is

ever reviewed by intelligence analysts." Shea Decl. ¶ 5. In 2012, fewer than 300 identifiers were queried. Shea Decl. ¶ 24. Because each query obtains information for contact numbers up to three hops out from the seed, the total number of responsive records was "substantially larger than 300, but . . . still a very small percentage of the total volume of metadata records." Shea Decl. ¶ 24. Between May 2006 and May 2009, the NSA provided the FBI and other agencies with 277 reports containing approximately 2,900 telephone numbers. Shea Decl. ¶ 26.

III. Plaintiffs' Claims

Plaintiffs filed this lawsuit on June 11, 2013, less than a week after the unauthorized disclosure of the Secondary Order. The ACLU, ACLU Foundation, NYCLU, and NYCLU Foundation are "non-profit organizations that engage in public education, lobbying, and pro bono litigation upholding the civil rights and liberties guaranteed by the Constitution." Compl. ¶ 24 (ECF No. 1). The ACLU and ACLU Foundation are Verizon subscribers and their telephony metadata is therefore subject to the Secondary Order. Compl. ¶¶ 28, 35. The NYCLU was a Verizon subscriber until early April 2013. Compl. ¶ 29. The NYCLU and NYCLU Foundation alleges that their metadata was collected under a previous order before the expiration of its Verizon contract. Compl. ¶ 3, 35. The ACLU and ACLU Foundation are also customers of Verizon Wireless and allege that similar orders were provided to Verizon Wireless, allowing the Government to obtain information concerning calls placed or received on the mobile telephones of ACLU employees. Compl. ¶¶ 28, 35. While the Secondary Order does not cover calls placed on Verizon Wireless's network, the Government acknowledged that it has collected metadata for substantially every telephone call in the United States since May 2006. See Shea Decl. ¶ 13; White Paper at 3.

The Plaintiffs' employees routinely communicate by telephone with each other as well as with journalists, clients, legislators, and members of the public. The Plaintiffs' assert that "their" telephone records "could readily be used to identify those who contact Plaintiffs . . . and is likely to have a chilling effect." Compl. ¶ 35. The Plaintiffs' seek a declaratory judgment that the NSA's metadata collection exceeds the authority granted by section 215 and violates the First and Fourth Amendments, and it also seeks a permanent injunction enjoining the Government from continuing the collection. Compl. ¶¶ 36–38.

The Government moves to dismiss the complaint under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) for lack of standing and failure to state a claim. The ACLU moves under Rule 65 for a preliminary injunction barring the Government from "collecting [Plaintiffs'] call records" during the pendency of this action, requiring it to quarantine "all of [Plaintiffs'] call records [it] already collected," and enjoining the Government from querying metadata using any identifier associated with the Plaintiffs. Pls. Mot. For Prelim. Inj., dated Aug. 26, 2013 at 2 (ECF No. 26) [hereinafter "Pls. Mot."].

DISCUSSION

I. Standing

"[N]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies." DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 341 (2006) (internal quotation marks and alterations omitted); see also Rothstein v. UBS AG, 708 F.3d 82, 89–90 (2d Cir. 2013). The case-or-controversy requirement of Article III of the Constitution requires plaintiffs to establish their standing to sue. Amnesty Int'l, 133 S. Ct. at 1146 (citing Raines v. Byrd, 521

U.S. 811, 818 (1997)). "The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches." Amnesty Int'l, 133 S. Ct. at 1146. Therefore a court's standing inquiry is "especially rigorous" when the merits of the case would require the court "to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." Amnesty Int'l, 133 S. Ct. at 1147 (quoting Raines, 521 U.S. at 819–20).

Article III standing requires an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." Monsanto Co. v. Geertson Seed Farms, 130 S. Ct. 2743, 2752 (2010) (citing Horne v. Flores, 557 U.S. 433, 445(2009)). The ACLU alleges three sources of injury: (1) the Government's mere collection of the metadata related to the ACLU's telephone calls; (2) the "search" of metadata related to the ACLU's telephone calls that results when any seed is queried because the NSA must check all of the metadata it has collected to identify all telephone numbers within three hops of the seed; and (3) the chilling effect on potential ACLU clients, whistleblowers, legislators, and others who will hesitate to contact the ACLU by telephone because they know the NSA will have a record that the call occurred.

Relying on the Supreme Court's decision in Clapper v. Amnesty International, 133 S. Ct. 1138, the Government contends that none of these alleged injuries are "concrete, particularized, and actual or imminent." Monsanto, 130 S. Ct. at 2752. Amnesty International was a facial challenge to the FISA Amendments Act of 2008, which expanded the Government's authority to intercept the contents of communications for foreign intelligence purposes. The Amnesty International plaintiffs included attorneys and human rights organizations whose work

required them to communicate with individuals overseas who might be targets of Government surveillance under the FISA Amendments Act, such as Guantanamo detainees. They alleged violations under the First and Fourth Amendments. While they offered no evidence their communications had in fact been intercepted, they asserted that there was an "objectively reasonable likelihood" their communications with foreign contacts would be intercepted in the future.[5] They also argued that they suffered a present injury stemming from expensive precautions they took to avoid interception, such as traveling overseas to meet their clients in person instead of communicating electronically.

The Supreme Court found the Amnesty International plaintiffs had suffered no injury in fact. The Court declined to assess standing based on an "'objectively reasonable likelihood' standard," finding it "inconsistent with [the] requirement that 'threatened injury must be certainly impending to constitute injury in fact.'" Amnesty Int'l, 133 S. Ct. at 1147 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)). The Amnesty International plaintiffs' "highly speculative fear" that their communications would be intercepted was insufficient to confer standing. Amnesty Int'l, 133 S. Ct. at 1148. In so holding, the Supreme Court deconstructed the Amnesty International plaintiffs "highly attenuated chain of possibilities":

(1) the Government will decide to target the communications of

[5] A panel in the Second Circuit adopted this novel view of standing. See Amnesty Int'l USA v. Clapper, 638 F.3d 118, 133-34, 139 (2d Cir. 2011), overruled by 133 S. Ct. 1138 (2013). This conclusion was criticized by other Second Circuit judges. See Amnesty Int'l USA v. Clapper, 667 F.3d 163, 194 (2d Cir. 2011) (denial of rehearing en banc) (Raggi, J. dissenting) (In finding that an "objectively reasonable likelihood" standard applied, "the panel did not explain its disregard of the Supreme Court's requirement that injury must be actual or imminently threatened"). The Supreme Court expressly rejected the Second Circuit's formulation. See Amnesty Int'l, 133 S. Ct. at 1146, 1151.

> non-U.S. persons with whom [the plaintiffs] communicate;[6]
>
> (2) in doing so, the Government will choose to invoke its authority under [the FISA Amendments Act] rather than utilizing another method of surveillance,
>
> (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy [the FISA Amendments Act's] many safeguards and are consistent with the Fourth Amendment;
>
> (4) the Government will succeed in intercepting the communications of respondents' contacts; and
>
> (5) respondents will be parties to the particular communications that the Government intercepts.

Amnesty Int'l, 133 S. Ct. at 1148. "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is certainly impending." Amnesty Int'l, 133 S. Ct. at 1147 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 564 n.2 (1992)) (emphasis in original).

The Amnesty International plaintiffs fared no better with their second alleged injury—costly precautions taken to avoid the risk of surveillance. In the Supreme Court's view, that the plaintiffs "incurred certain costs as a reasonable reaction to a risk of harm" was insufficient "because the harm [plaintiffs sought] to avoid [was] not certainly impending." Amnesty Int'l, 133 S. Ct. at 1151. "Because respondents do not face a threat of certainly impending interception under [the FISA Amendments Act], the costs that they have incurred to

[6] The Amnesty International plaintiffs were all U.S. persons. The FISA Amendments Act permits the NSA to intercept communications of U.S. persons only if they communicate with a non-U.S. person reasonably believed to be outside the United States who is the target of the surveillance. See Amnesty Int'l, 133 S. Ct. at 1144, 1148.

avoid surveillance are simply the product of their fear of surveillance . . . such a fear is insufficient to create standing." Amnesty Int'l, 133 S. Ct. at 1152 (citing Laird v. Tatum, 408 U.S. 1, 10–15 (1972)).

Amidax Trading Group v. S.W.I.F.T. SCRL, 671 F.3d 140 (2d Cir. 2011) is instructive. Amidax's bank used SWIFT[7] to transfer funds among financial institutions. After the September 11th attacks, the Office of Foreign Assets Control subpoenaed SWIFT's records to monitor the financial transactions of suspected terrorists. Amidax sued SWIFT and the Government, alleging, inter alia, violations of the First and Fourth Amendments. The Second Circuit held that "[t]o establish an injury in fact—and thus, a personal stake in this litigation—[Amidax] need only establish that its information was obtained by the government." Amidax, 671 F.3d at 147 (alteration in original) (emphasis added) (quoting Amidax Trading Grp. v. S.W.I.F.T. SCRL, 607 F. Supp. 2d 500, 508 (S.D.N.Y. 2009)). But because Amidax could not plausibly show the Government had collected its records, it lacked standing. Amidax, 671 F.3d at 148–49.

Here, there is no dispute the Government collected telephony metadata related to the ACLU's telephone calls. Thus, the standing requirement is satisfied. See Amnesty Int'l, 133 S. Ct. at 1153 (noting that the case would be different if "it were undisputed that the Government was using [the FISA Amendments Act]-authorized surveillance to acquire respondents' communications and . . . the sole dispute concerned the reasonableness of respondents' preventive measures"); see also Klayman v. Obama, --- F. Supp. 2d ----, 2013 WL 6571596, at

[7] SWIFT stands for Society for Worldwide Interbank Financial Telecommunication. It provides electronic instructions on how to transfer money among thousands of financial institutions worldwide. See Amidax, 671 F.3d at 143.

*14–17 (D.D.C. Dec. 16, 2013) (finding standing for subscriber to challenge the NSA telephony metadata collection program).

The Government argues that merely acquiring an item does not implicate a privacy interest, but that is not an argument about Article III standing. Rather, it speaks to the merits of a Fourth Amendment claim. Cf. Rakas v. Illinois, 439 U.S. 128, 139 (1978) ("Rigorous application of the principle that the rights secured by the [Fourth] Amendment are personal, in place of a notion of "standing" will produce no additional situations in which evidence must be excluded. . . . [T]he better analysis . . . focuses on the extent of particular [individual's Fourth Amendment] rights, rather than on any theoretically separate, but invariably intertwined concept of standing.") The ACLU is not obligated at the standing stage to prove the merits of its case, only that it has "a personal stake in this litigation." Amidax, 671 F.3d at 147. Because the ACLU has alleged an actual injury grounded in the Government's collection of metadata related to its telephone calls, it has standing.

II. Statutory Claim

A. Sovereign Immunity

The United States, as sovereign, is immune from suit unless it unequivocally consents to being sued. United States v. Mitchell, 445 U.S. 535, 538 (1980); see also Price v. United States, 174 U.S. 373, 375-76 (1899) ("It is an axiom of our jurisprudence. The government is not liable to suit unless it consents thereto, and its liability in suit cannot be extended beyond the plain language of the statute authorizing it."). Section 702 of the Administrative Procedure Act ("APA") waives sovereign immunity for suits against the United States that, like this one, seek "relief other than money damages." 5 U.S.C. § 702. The APA

creates a "strong presumption that Congress intends judicial review of administrative action." Bowen v. Mich. Acad. of Family Physicians, 476 U.S. 667, 670 (1986).

Exceptions to the APA's broad waiver are "construed narrowly and apply only if there is 'clear and convincing evidence of legislative intention to preclude review.'" Nat. Res. Def. Council v. Johnson, 461 F.3d 164, 171 (2d Cir. 2006) (quoting Japan Whaling Ass'n v. Am. Cetacean Soc'y, 478 U.S. 221, 230 n.4 (1986)). But the presumption favoring judicial review, "like all presumptions used in interpreting statutes, may be overcome by specific language or specific legislative history that is a reliable indicator of congressional intent." Block v. Cmty. Nutrition Inst., 467 U.S. 340, 349 (1984). In particular, "the presumption favoring judicial review of administrative action may be overcome by inferences of intent drawn from the statutory scheme as a whole." Block, 467 U.S. at 349.

1. Section 702 Exception

Section 702 does not "confer[] authority to grant relief if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought." 5 U.S.C. § 702. This carve out ensures that a plaintiff cannot "exploit[] the APA's waiver to evade limitations on suit contained in other statutes" because "[t]he waiver does not apply 'if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought' by the plaintiff." Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak, 132 S. Ct. 2199, 2204–05 (2012). Thus, "'[w]hen Congress has dealt in particularity with a claim and [has] intended a specified remedy' . . . to be exclusive, that is the end of the matter; the APA does not undo the judgment." Pottawatomi Indians, 132 S. Ct. at 2205 (alterations in original) (quoting Block v. North Dakota ex rel. Bd. of Univ. & Sch. Lands, 461 U.S. 273, 286 n.22 (1983)).

The PATRIOT Act reengineered various provisions of the Wiretap Act, the Stored Communications Act, and FISA. Section 223 of the PATRIOT Act amended the Wiretap Act and the Stored Communications Act to remove the United States as a party that could be sued by an aggrieved person under those statutes. Pub. L. No. 107-56 § 223, 115 Stat. 272 (2001) (amended 18 U.S.C. § 2520(a) and 18 U.S.C. § 2707(a) to insert "other than the United States"); Jewel v. Nat'l Sec. Agency, --- F. Supp. 2d ----, 2013 WL 3829405, at *12 (N.D. Cal. July 23, 2013) (section 223 "explicitly deleted the United States from the provisions that permit an aggrieved person to sue for recovery and obtain relief, including 'preliminary and other equitable or declaratory relief [with respect to the Wiretap Act and the Stored Communications Act].'"). At the same time, section 223 created a limited right to sue the United States for money damages for claims arising out of the Wiretap Act, the Stored Communications Act, and FISA. Specifically, part of section 223 was codified as Title 18, United States Code, Section 2712, titled "Civil actions against the United States" and is the "exclusive remedy against the United States for any claims within the purview of this section." 18 U.S.C. § 2712(d). Section 2712 allows a plaintiff to recover money damages for any "willful violation" of the Wiretap Act, the Stored Communications Act, and three provisions of FISA: (1) electronic wiretap surveillance; (2) physical searches; and (3) pen registers or trap and trace devices. 18 U.S.C. § 2712(a).

The operation of section 223—excising non-damage suits from the Wiretap Act and the Stored Communications Act and designating section 2712 as the only avenue for a civil action under the Wiretap Act, the Stored Communications Act and certain FISA sections—shows Congress's intent to permit only money damages suits under the limited circumstances delineated in section 2712. See Jewel, 2013 WL 3829405, at *12. It is unsurprising that section

2712 does not authorize monetary damage suits for section 215 violations. Congress's concern was to provide redress for privacy violations where the Government took action to generate evidence—such as electronic eavesdropping, physical searches, or the installation of pen registers or trap and trace devices[8]—but provided no statutory cause of action when evidence was created solely in the ordinary course of business of a third party.

This interpretation of section 215 is buttressed by FISA's overall statutory scheme: in contrast to other FISA surveillance statutes, section 215 does not authorize any action for misuse of the information obtained. Compare 50 U.S.C. § 1861 (use of information obtained from "tangible things" order not subject to redress under section 2712) with 50 U.S.C. § 1806(a) (use of information obtained from electronic surveillance actionable under section 2712); 50 U.S.C. § 1825(a) (same for physical searches); 50 U.S.C § 1845(a) (same for pen registers and trap and trace devices). Thus, Congress withdrew the APA's waiver of sovereign immunity for section 215. See Pottawatomi Indians, 132 S. Ct. at 2204–05; see also Klayman, 2013 WL 6571596, at *12 n.30; Jewel, 2013 WL 3829405, at *12.

2. Section 701 Exception

Section 701 of the APA withdraws the immunity waiver "to the extent the relevant statute 'preclude[s] judicial review.'" Block, 467 U.S. at 345 (alterations in original) (citing 5 U.S.C. § 701(a)(1)). "Whether and to what extent a particular statute precludes judicial review is determined not only from its express language, but also from the structure of the statutory scheme, its objectives, its legislative history, and the nature of the administrative action

[8] Pen register and trap and trace devices are electronic devices that, respectively, record all call detail information for telephone numbers called from or to a particular telephone line. However, they do not capture the content of the call. See 18 U.S.C. § 3127(3)-(4).

involved." Block, 467 U.S. at 345.

In Block, the Supreme Court held that a milk consumer's challenge to milk market orders issued under the Agricultural Marketing Agreement Act was precluded under APA section 701(a)(1). 467 U.S. at 347. As the Supreme Court explained, the Agricultural Marketing Agreement Act "contemplates a cooperative venture" between the Secretary of Agriculture, milk handlers, and milk producers. Block, 467 U.S. at 346. For example, the Agricultural Marketing Agreement Act provides for "agreements among the Secretary, producers, and handlers, for hearings among them, and for votes by producers and handlers." Block, 467 U.S. at 346–47 (internal citations omitted). The Agricultural Marketing Agreement Act requires a handler to exhaust administrative remedies before it permitted any judicial review. Block, 467 U.S. at 346. But the Agricultural Marketing Agreement Act was silent regarding milk consumers' remedies.

The Supreme Court found that silence, coupled with the statutory scheme, demonstrated that milk consumers' claims were precluded. Although the Agricultural Marketing Agreement Act impacted consumer interests, the Court concluded that "the preclusion issue does not only turn on whether the interests of a particular class . . . are implicated," rather, it turns on whether "Congress intended for that class to be relied upon to challenge agency disregard of the law." Block, 467 U.S. at 347. The Court went on to find that "[i]n a complex scheme of this type, the omission of such a provision is sufficient reason to believe that Congress intended to foreclose consumer participation in the regulatory process." Block, 467 U.S. at 347. "[W]hen a statute provides a detailed mechanism for judicial consideration of particular issues at the behest of particular persons, judicial review of those issues at the behest of other persons may be found to be impliedly precluded." Block, 467 U.S. at 349.

The interplay between section 215 and FISA's statutory scheme compel the same conclusion here. Section 215 expressly provides that "[a] person receiving a production order may challenge the legality of that order by filing a petition with the pool [of FISC judges] established by section 1803(e)(1) of this title." 50 U.S.C. § 1861(f)(2)(A)(i). It also prohibits any non-FISC modification of section 215 orders: "[a]ny production or nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect." 50 U.S.C. § 1861(f)(2)(D). Like the statutory scheme in Block, section 215 does not provide for any person other than a recipient of an order to challenge the orders' legality or otherwise participate in the process. See Ark. Dairy Coop. Ass'n, Inc. v. U.S. Dep't of Agr., 573 F.3d 815, 822 (D.C. Cir. 2009) (In Block, "the Supreme Court did not concentrate simply on the presence or absence of an explicit right [to appeal a milk market order] but instead noted that in the 'complex scheme' of the Agricultural Marketing Agreement Act, there was no provision for consumer participation of any kind.").

The "cooperative venture" envisioned by FISA's statutory scheme does not involve a mundane subject like milk pricing—it involves national security, a matter of vital importance. Congress's intent to keep the means and methods of the Government's intelligence gathering efforts secret from its enemies lies at the heart of FISA. Section 215 limits disclosure of orders to the narrowest group of individuals: (1) those to whom disclosure is necessary to comply with such an order; (2) an attorney to obtain legal advice on how to respond to the order;

and (3) other persons as permitted by the Director of the FBI. See 50 U.S.C. § 1861(d).[9] Section 215 does not just exclude a target from challenging an order, it precludes their participation in any way. See Ark. Dairy Coop. Ass'n, 573 F.3d at 822; Block, 467 U.S. at 346).

Allowing any challenge to a section 215 order by anyone other than a recipient would undermine the Government's vital interest in keeping the details of its telephone metadata collection program secret. It would also—because of the scope of the program—allow virtually any telephone subscriber to challenge a section 215 order. In Koretoff v. Vilsack, 614 F.3d 532, 537, (D.C. Cir. 2011) the D.C. Circuit discussed such an absurdity that also cropped up in Block. The D.C. Circuit noted that "[a]llowing suit by consumers would mean virtually every American could challenge every agricultural marketing order. . . . [T]hat hard-to-fathom result was of great concern to the Supreme Court [in Block] and informed its assessment of Congress's intent on whether such suits were precluded by the [Agricultural Marketing Agreement Act]." Koretoff, 614 F.3d at 537. Allowing anyone but the recipient of section 215 orders to challenge them, or to do so anywhere outside the FISC, "would severely disrupt this complex and delicate administrative scheme." Block, 467 U.S. at 348. It is clear from the statutory scheme that Congress intended to preclude statutory causes of action such as this.

Of course, this says nothing about the ACLU's constitutional claims and it is hard

[9] During the 2005 reauthorization of section 215, Congressman Nadler offered an amendment in the Judiciary Committee that would have permitted the recipient of an order to challenge compliance in a district court. In his remarks, Congressman Nadler stated, "[This amendment] allows the recipient of a section 215 order to challenge the order in [a district] court. This is a common-sense protection that is sorely lacking in the current law. Now the recipient, not the target—this isn't good enough, but we can't do the target. . . . It doesn't give the target of the order the ability to go to court. He doesn't know about it. But the recipient, if they wish, can challenge it in court." H.R. Rep. 109-174, pt 1, at 128. That amendment failed. H.R. Rep. 109-174, pt 1, at 47.

to image a regime where they would be barred. A constitutional claim is precluded only on a "heightened showing" demonstrating a clear intent to do so. Webster v. Doe, 486 U.S. 592, 603 (1988). And there is no language in FISA expressly barring a constitutional claim. See Klayman, 2013 WL 6571596, at *13.

Regarding the statutory arguments, there is another level of absurdity in this case. The ACLU would never have learned about the section 215 order authorizing collection of telephony metadata related to its telephone numbers but for the unauthorized disclosures by Edward Snowden. Congress did not intend that targets of section 215 orders would ever learn of them. And the statutory scheme also makes clear that Congress intended to preclude suits by targets even if they discovered section 215 orders implicating them. It cannot possibly be that lawbreaking conduct by a government contractor that reveals state secrets—including the means and methods of intelligence gathering—could frustrate Congress's intent. To hold otherwise would spawn mischief: recipients of orders would be subject to section 215's secrecy protocol confining challenges to the FISC, while targets could sue in any federal district court. A target's awareness of section 215 orders does not alter the Congressional calculus. The ACLU's statutory claim must therefore be dismissed.

B. Merits of the Statutory Claims

Even if the statutory claim were not precluded, it would fail. "A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." Winter v. NRDC, 555 U.S. 7, 20 (2008) (citing Munaf v. Geren, 553 U.S. 674, 689–90 (2008)); see also N.Y. Progress & Prot.

PAC v. Walsh, 733 F.3d 483, 486 (2d Cir. 2013). Here, the ACLU fails to demonstrate a likelihood of success on the merits of their statutory claim.

1. Does the Stored Communications Act Prohibit the Collection of Telephony Metadata Under Section 215?

Section 215 was enacted at the same time as an amendment to the Stored Communications Act. As amended, the Stored Communications Act prohibits communications providers from "knowingly divulg[ing]" a subscriber's records to a government entity unless one of several exceptions are met. 18 U.S.C. § 2702(a)(3). These include when the Government obtains a warrant, an administrative subpoena, a grand jury or trial subpoena, or an order issued under § 2703(d). 18 U.S.C. § 2703(c). The Government may also obtain telephony metadata with a national security letter ("NSL") issued under 18 U.S.C. § 2709.[10] An NSL does not require judicial approval. The only hurdle is a certification from the Director of the FBI or his designee 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)(1).

By contrast, section 215 allows the government an order "requiring the production of any tangible thing." Prior to its amendment, the Government's FISA authority to collect business records applied only to records from "common carrier[s], public accommodation facilit[ies], physical storage facilit[ies], or vehicle facilit[ies]." 50 U.S.C. § 1862 (2001). Section 215 broadened the Government's authority to seek records from additional businesses. See 50 U.S.C § 1861 (as amended, 2008). The only limitation--relevant here—on the types of records that may be obtained with a section 215 order are that they be obtainable with a grand

[10] An NSL is an administrative subpoena, which is one of the SCA's listed exceptions. See 18 U.S.C. § 2703(c)(2).

jury subpoena. See 50 U.S.C. § 1861(c)(2)(D). Section 215 contains nothing suggesting that it is limited by the Stored Communications Act. Nevertheless, Plaintiffs argue that section 215 should be interpreted narrowly to avoid any conflict with the Stored Communications Act.

But this court must attempt to interpret a statute "as a symmetrical and coherent regulatory scheme, and fit, if possible, all parts into an harmonious whole" and is "guided to a degree by common sense." Food & Drug Admin. v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000). Read in harmony, the Stored Communications Act does not limit the Government's ability to obtain information from communications providers under section 215 because section 215 orders are functionally equivalent to grand jury subpoenas. Section 215 authorizes the Government to seek records that may be obtained with a grand jury subpoena, such as telephony metadata under the Stored Communications Act.

That conclusion is bolstered by common sense: to allow the Government to obtain telephony metadata with an NSL but not a section 215 order would lead to an absurd result. Unlike an NSL, a section 215 order requires a FISC judge to find the Government has provided a "statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant" to a foreign intelligence investigation. 50 U.S.C. § 1861(b)(2)(A). As FISC Judge Walton found,

> [i]t would have been anomalous for Congress, in enacting the USA PATRIOT Act, to have deemed the FBI's application of a 'relevance' standard, without prior judicial review, sufficient to obtain records subject to [the Stored Communications Act], but to have deemed the FISC's application of a closely similar 'relevance' standard insufficient for the same purpose. This anomaly is avoided by interpreting sections 2702–2703 as implicitly permitting the production of records pursuant to a FISC order issued under [section 215].

In re Prod. of Tangible Things from [REDACTED], No. BR 08-13, Supp. Op. at 5 (F.I.S.C. Dec. 12, 2008) (emphasis in the original). Any dissonance between the two provisions melts away when the Stored Communications Act is read as permitting section 215 orders to obtain telephony metadata.

2. Did Congress Ratify The Government's Interpretation of Section 215?

"Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change." Forest Grove Sch. Dist. v. T.A., 557 U.S. 230, 239–40 (2009) (quoting Lorillard v. Pons, 434 U.S. 575, 580 (1978)). "When 'all (or nearly all) of the' relevant judicial decisions have given a term or concept a consistent judicial gloss, we presume Congress intended the term or concept to have that meaning when it incorporated it into a later-enacted statute." Bruesewitz v. Wyeth LLC, 131 S. Ct. 1068, 1082 (2011) (citing Merck & Co. v. Reynolds, 130 S. Ct. 1784, 1802 (2010)). "The consistent gloss represents the public understanding of the term." Bruesewitz, 131 S. Ct. at 1082.

The Government argues Congress was aware of the bulk metadata collection program and ratified it by reenacting section 215. Before Congress reauthorized FISA, no judicial opinion interpreting relevance was public, which was in line with Congress's design. Congress passed FISA to engraft judicial and congressional oversight onto Executive Branch activities that are most effective when kept secret. To conduct surveillance under section 215, the Executive must first seek judicial approval from the FISC. See 50 U.S.C. § 1861. Then, on a semi-annual basis, it must provide reports to the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the

Committees on the Judiciary of the House of Representatives and the Senate. 50 U.S.C. § 1871. Those Congressional reports must include: (1) a summary of significant legal interpretations of section 215 involving matters before the FISC; and (2) copies of all decisions, orders, or opinions of the FISC that include significant construction or interpretation of section 215. 50 U.S.C. § 1871.

The Congressional reports are not public and are submitted "in a manner consistent with the protection of the national security," namely, in classified, secret proceedings. 50 U.S.C. § 1871. Such Congressional proceedings are akin to application process for a section 215 order and the FISC opinions on those applications—they are all classified, secret proceedings. There is no doubt that the Congressional Committees responsible for oversight of this program knew about the FISC opinions and the Executive Branch's interpretation of section 215. But what about the rest of Congress?

In 2010 and 2011, Congress reauthorized section 215 without making any changes.[11] Prior to the 2010 reauthorization, the Executive Branch made available to all members of Congress a classified, five-page document discussing the bulk telephony metadata program. On February 23, 2010, Senators Feinstein and Bond wrote to their colleagues:

> Members of the Select Committee on Intelligence have previously requested that the Executive Branch permit each Member of Congress access to information on the nature and significance of intelligence authority on which they are asked to vote. In response to these requests, the Attorney General and the Director of National Intelligence have provided a classified paper to the House

[11] An Act to Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, Pub. L. No. 111-141, 124 Stat. 37 (2010); FISA Sunsets Extension Act of 2011, Pub. L. No. 112-3, 125 Stat. 5 (2011); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011).

> and Senate Intelligence Committees on important intelligence collection made possible by authority that is subject to the approaching sunset, and asked for our assistance in making it available, in a secure setting, directly and personally to any interested Member.

Letter from Sens. Feinstein & Bond to Colleagues (Feb. 23, 2010) (ECF No. 33-6). Representative Reyes addressed a similar letter to his House colleagues. See Letter from Rep. Reyes to Colleagues (Feb. 24, 2010) (ECF No. 33-7).

That classified document, which was made available prior to the vote for reauthorization and has now been declassified in part, informed the reader that "[section 215] orders generally require production of the business records . . . relating to substantially all of the telephone calls handled by the [telecommunications] companies, including both calls made between the United States and a foreign country and calls made entirely within the United States." NSA Report.

The following year, when section 215 was again scheduled to sunset, senators were informed of an updated classified document available for their review. See Letter from Sens. Feinstein & Chambliss to Colleagues (Feb. 8, 2011) (ECF No. 33-11). Apparently some

Senators did review it,[12] while other Members of Congress did not.[13] The House Intelligence Committee did not make the document available to members of the House. Dozens of House members elected in 2010 therefore never had an opportunity to review the classified document. While this is problematic, the Executive Branch did what it was required to do under the statutory scheme that Congress put in place to keep Congress informed about foreign intelligence surveillance.

And viewing all the circumstances presented here in the national security context, this Court finds that Congress ratified section 215 as interpreted by the Executive Branch and the FISC, when it reauthorized FISA. In cases finding ratification, it is fair to presume that Congress had knowledge of the statute's interpretation. See Forest Grove Sch. Dist., 557 U.S. at 239–40 (Congress is presumed to be aware of Supreme Court decision); Lorillard, 434 U.S. at 580–81

---

[12] For example, Senator Wyden stated, "[M]any Members of Congress have no idea how the law is being secretly interpreted by the Executive Branch." and Senator Udall echoed that sentiment: "[W]hat most people—including many Members of Congress—believe the PATRIOT Act allows the government to do . . . and what government officials privately believe the PATRIOT Act allows them to do are two different things." See 157 Cong. Rec. S3386 (daily ed. May 26, 2011). At the time, Senators Wyden and Udall's remarks precipitated a Freedom of Information Act lawsuit by The New York Times seeking disclosure of the classified report to Congress. That case was assigned to this Court. After briefing, argument, and an in camera review, this Court concluded that disclosure of the report would "enable America's adversaries to develop means to degrade and evade the nation's foreign intelligence collection capabilities" and that it would "reveal and potentially compromise intelligence sources and methods." N.Y. Times Co. v. U.S. Dep't of Justice, 872 F. Supp. 2d 309, 316-17 (S.D.N.Y. 2012).

[13] Congressman Sensenbrenner asserts in an amicus brief that "he was not aware of the full scope of the [telephony metadata collection] program when he voted to reauthorize section 215" and that "had he been fully informed he would not have voted to reauthorize section 215 without change." Br. of Amicus Curiae, F. James Sensenbrenner ("Amicus Br.")at 9-10 (ECF No. 56). This is a curious statement: Congressman Sensenbrenner not only had access to the five-page report made available to all Congressmen, but he also, as "a long-serving member of the House Judiciary Committee", "Amicus Br. at 1, was briefed semi-annually by the Executive Branch that included "a summary of significant legal interpretations of section 215 involving matters before the FISC" and "copies of all decisions, orders, or opinions of the FISC that include significant construction or interpretation of section 215." 50 U.S.C. § 1871.

(Congress is presumed to be aware that "every court to consider the issue" has held there is a right to a jury trial in FLSA actions); Butterbaugh v. Dep't of Justice, 336 F.3d 1332, 1342 (Fed. Cir. 2003) (congressional awareness shown by "[e]xtensive hearings, repeated efforts at legislative correction, and public controversy"); cf. Comm'r of Internal Revenue v. Glenshaw Glass Co, 348 U.S. 426, 431 (1955) (declining to find ratification where there is not "the slightest affirmative indication that Congress ever had the [relevant] decision before it").

3. Is Bulk Telephony Metadata Collection Permitted By Section 215?

To obtain a section 215 order, the Government must show (1) "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation" and (2) that the item sought must be able to be "obtained with a subpoena duces tecum . . . in aid of a grand jury investigation or with any other [court] order . . . directing the production of records or tangible things." 50 U.S.C. § 1861(b)-(c). The Government can obtain telephony metadata with grand jury subpoenas and other court orders. See 18 U.S.C. § 2703(c)-(d).

A grand jury subpoena permits the Government to obtain tangible things unless "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation." United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991). The ACLU argues that the category at issue—all telephony metadata—is too broad and contains too much irrelevant information. That argument has no traction here. Because without all the data points, the Government cannot be certain it connected the pertinent ones. As FISC Judge Eagan noted, the collection of virtually all telephony metadata is "necessary" to permit the NSA, not the FBI, to do the algorithmic data analysis that allow the NSA to determine "connections between known and unknown

international terrorist operatives." In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], amended slip op. at 22–23. And it was the FISC that limited the NSA's production of telephony metadata to the FBI. While section 215 contemplates that tangible items will be produced to the FBI, FISC orders require that bulk telephony metadata be produced directly—and only—to the NSA. And the FISC forbids the NSA from disseminating any of that data until after the NSA has identified particular telephony metadata of suspected terrorists. Without those minimization procedures, FISC would not issue any section 215 orders for bulk telephony metadata collection. In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], amended slip op. at 23.

"Relevance" has a broad legal meaning. The Federal Rules of Civil Procedure allow parties to obtain discovery "regarding any nonprivileged matter that is relevant to any party's claim or defense." Fed. R. Civ. P. 26(b)(1) (emphasis added). This Rule "has been construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case." Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 351 (1978) (citing Hickman v. Taylor, 329 U.S. 495, 501 (1947)). Tangible items are "relevant" under section 215 if they bear on or could reasonably lead to other matter that could bear on the investigation.

Under section 215, the Government's burden is not substantial. The Government need only provide "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant." 50 U.S.C. § 1861(b)(2)(A) (emphasis added). Because section 215 orders flow from the Government's grand jury and administrative subpoena powers,

see 50 U.S.C. § 1861, the Government's applications are subject to deferential review. See R. Enters., Inc., 498 U.S. at 301 (upholding grand jury subpoena challenged on relevancy grounds unless "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation"); Nat'l Labor Relations Bd. v. Am. Med. Response, Inc., 438 F.3d 188, 193 (2d Cir. 2006) (finding that for an administrative subpoena, "the agency's appraisal of relevancy" to its investigation " must be accepted so long as it is not obviously wrong"). FISA applications for section 215 orders "are subject to 'minimal scrutiny by the courts,' both upon initial presentation and subsequent challenge." United States v. Abu-Jihaad, 630 F.3d 102, 130 (2d Cir. 2010) (quoting United States v. Duggan, 743 F.3d 59, 77 (2d Cir. 1984)).

The concept of relevance in the context of an investigation does not require the Government to parse out irrelevant documents at the start of its investigation. Rather, it allows that Government to get a category of materials if the category is relevant. The question of the permissible scope is generally "variable in relation to the nature, purposes and scope of the inquiry." Okla. Press Pub. Co. v. Walling, 327 U.S. 186, 209 (1946). Defining the reasonableness of a subpoena based on the volume of information to be produced would require the Government to determine wrongdoing before issuing a subpoena—but that determination is the primary purpose for a subpoena. See Okla. Press Pub. Co., 327 U.S. at 201 (noting that administrative subpoenas are authorized "to discover and procure evidence, not to prove a pending charge or complaint, but upon which to make one"). And in the context of a counterterrorism investigation, that after-the-attack determination would be too late.

Here, there is no way for the Government to know which particle of telephony metadata will lead to useful counterterrorism information.[14] When that is the case, courts routinely authorize large-scale collections of information, even if most of it will not directly bear on the investigation. See In re Subpoena Duces Tecum, 228 F.3d 341, 350–51 (4th Cir. 2000) (authorizing collection of 15,000 patient files); In re Grand Jury Proceedings: Subpoena Duces Tecum, 827 F.2d 301 (8th Cir. 1987) (authorizing collection of all wire transactions over $1,000 for a 14-month period at a particular Western Union office).

Any individual call record alone is unlikely to lead to matter that may pertain to a terrorism investigation. Approximately 300 seeds were queried in 2012 and only a "very small percentage of the total volume of metadata records" were responsive to those queries." Shea Decl. ¶ 24. But aggregated telephony metadata is relevant because it allows the querying technique to be comprehensive. And NSA's warehousing of that data allows a query to be instantaneous. This new ability to query aggregated telephony metadata significantly increases the NSA's capability to detect the faintest patterns left behind by individuals affiliated with foreign terrorist organizations. Shea Decl. ¶¶ 46, 48. Armed with all the metadata, NSA can draw connections it might otherwise never be able to find.[15]

---

[14]There is no question that "individuals associated with international terrorist organizations use telephonic systems to communicate with one another around the world, including the United States. In re Application, amended slip op. at 21. And the Government "'[a]nalysts know that the terrorists' communications are located somewhere' in the metadata [database], but cannot know where until the data is aggregated and then [queried.]" In re Application, amended slip op. at 21.

[15] Prior to September 11th, NSA did not have that capability. General Alexander summed it up aptly, "We couldn't connect the dots because we didn't have the dots." Testimony before the House Permanent Select Committee on Intelligence, dated Jun. 18, 2013, General Keith Alexander, Director of the NSA, at 61 (ECF No. 33-13) [hereinafter "Alexander Testimony"].

The collection is broad, but the scope of counterterrorism investigations is unprecedented. National security investigations are fundamentally different from criminal investigations. They are prospective—focused on preventing attacks—as opposed to the retrospective investigation of crimes. National security investigations span "long periods of time and multiple geographic regions." Decl. of Robert J. Holley, FBI Acting Assistant Director of the Counterterrorism Division, dated Oct. 1, 2013, ¶ 18 (ECF No. 62). Congress was clearly aware of the need for breadth and provided the Government with the tools to interdict terrorist threats.

Relying on In re Horowitz, the ACLU's argues that the bulk telephony metadata collection program is overbroad because section 215 orders cover large volumes of irrelevant documents. Horowitz involved an investigation into financial crimes spanning borders and decades—and so the scope of the grand jury subpoena was necessary broad. In re Horowitz, 482 F.2d 72, 79–80 (2d Cir. 1973). After noting that "the failure to limit the subpoena by subject matter is not necessarily fatal," Judge Friendly narrowed the subpoena at issue to exclude categories documents that "have no conceivable relevance to any legitimate object of investigation by the federal grand jury." Horowitz, 482 F.2d at 79–80. He was troubled, in particular, with a subpoena that "require[d] production of all documents contained in the files, without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period." Horowitz, 482 F.2d at 79. The Second Circuit's exclusion of irrelevant categories of documents in Horowitz has no application here because telephony metadata is a category of relevant data. Any subpoena that seeks to obtain categories of

documents will likely return irrelevant documents—but only that portion of a subpoena seeking an irrelevant category of documents should be quashed.

Similarly, the ACLU reliance on In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993, 846 F. Supp. 11 (S.D.N.Y. 1994) is misplaced. There, Judge Mukasey was asked to decide whether to quash a subpoena directing a party to produce computer storage devices, not categories of documents within them. Judge Mukasey recognized that a "wider grand jury investigation into obstruction and related charges indeed justifies a commensurately broader subpoena" but cannot "justify a subpoena which encompasses documents completely irrelevant to its scope, particularly because the Government has acknowledged that relevant documents can be isolated through key-word searching." In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993, 846 F. Supp. at 13. Because the Government was unwilling to modify the subpoena, Judge Mukasey quashed it, concluding that "the subpoena at issue unnecessarily demands documents that are irrelevant to the grand jury inquiry." In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993, 846 F. Supp. at 13–14. Like In re Horowitz, this reasoning is no bar here because all telephony metadata is a relevant category of information.

III. Constitutional Claims

That Congress precluded the ACLU's statutory claims does not bar its constitutional ones. "[A] complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). To determine plausibility, courts follow a "two-pronged approach." Iqbal, 556 U.S. at 679. "First, although a court must

accept as true all of the allegations contained in a complaint, that tenet is inapplicable to legal conclusions, and threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." Harris v. Mills, 572 F.3d 66, 72 (2d Cir. 2009) (internal punctuation omitted). Second, a court determines "whether the 'well-pleaded factual allegations,' assumed to be true, 'plausibly give rise to an entitlement to relief.'" Hayden v. Paterson, 594 F.3d 150, 161 (2d Cir. 2010) (quoting Iqbal, 556 U.S. at 679). On a motion to dismiss, courts may consider "facts stated on the face of the complaint, in the documents appended to the complaint or incorporated in the complaint by reference, and . . . matters of which judicial notice may be taken." Allen v. WestPoint-Pepperell, Inc., 945 F.2d 40, 44 (2d Cir. 1991).

For the purposes of deciding the Government's motion to dismiss, this Court does not consider the affidavits submitted in conjunction with the ACLU's motion for a preliminary injunction. Chandler v. Coughlin, 763 F.2d 110, 113 (2d Cir. 1985) (error to consider affidavits in support of preliminary injunction in ruling on motion to dismiss); see also MacDonald v. Safir, 206 F.3d 183, 191 n.3 (2d Cir. 2000).

A. Fourth Amendment

The Fourth Amendment guarantees that all people shall be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. "[T]he Fourth Amendment protects people, not places." Katz v. United States, 389 U.S. 347, 351 (1967). A "search" occurs for purposes of the Fourth Amendment when the Government violates a person's "reasonable expectation of privacy." Katz, 389 U.S. at 360–61 (Harlan, J., concurring); see also United States v. Jones, 132 S. Ct. 945, 950 (2012); Bond v.

United States, 529 U.S. 334, 337 (2000).

In Smith v. Maryland, 442 U.S. 735 (1979), the Supreme Court held individuals have no "legitimate expectation of privacy" regarding the telephone numbers they dial because they knowingly give that information to telephone companies when they dial a number. 442 U.S. at 742. Smith's bedrock holding is that an individual has no legitimate expectation of privacy in information provided to third parties.[16]

Smith arose from a robbery investigation by the Baltimore police. Smith, 442 U.S. at 737. Without a warrant, the police requested that the telephone company install a device known as a pen register, which recorded the numbers dialed from Smith's home. Smith, 442 U.S. at 737. After Smith's arrest, he moved to suppress evidence derived from the pen register. Smith, 442 U.S. at 737. Noting it had consistently "held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," Smith, 442 U.S. at 743–44, the Court found that telephone customers have no subjective expectation of privacy in the numbers they dial because they convey that information to the telephone company knowing that the company has facilities to make permanent records of the numbers they dial. Smith, 442

[16] Here are just a few matters in which an individual has no constitutionally protected expectation of privacy. See, e.g., United States v. Miller, 425 U.S. 435, 441-43 (1976) (bank records); Couch v. United States, 409 U.S. 322, 335-36 (1973) (records given to accountant); Hoffa v. United States, 385 U.S. 293, 302-03 (1966) (information revealed to a confidant); On Lee v. United States, 343 U.S. 747, 971 (1952) (information revealed to a false friend); see also United States v.Todisco, 667 F.2d 255, 258 (2d Cir. 1981) (telephone numbers collected by a pen register). And some more recent iterations. See, e.g., United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (subscriber information provided to an internet service provider); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (information from a home computer that is transmitted over the Internet or by email); see also United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (information provided to Facebook "friend"). For an excellent discussion on the third party doctrine, see generally, Orin S. Kerr, The Case for the Third Party Doctrine, 107 Mich. L. Rev. 561 (2009).

U.S. at 742–43.

The privacy concerns at stake in Smith were far more individualized than those raised by the ACLU. Smith involved the investigation of a single crime and the collection of telephone call detail records collected by the telephone company at its central office, examined by the police, and related to the target of their investigation, a person identified previously by law enforcement. See Smith, 442 U.S. at 737. Nevertheless, the Supreme Court found there was no legitimate privacy expectation because "[t]elephone users . . . typically know that they must convey numerical information to the telephone company; that the telephone company has facilities for recording this information; and that the telephone company does in fact record this information for a variety of legitimate business purposes." Smith, 442 U.S. at 743; see also, e.g., United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009) (finding that because "data about the 'call origination, length, and time of call' . . . is nothing more than pen register and trap and trace data, there is no Fourth Amendment 'expectation of privacy.'") (citation omitted).

The ACLU argues that analysis of bulk telephony metadata allows the creation of a rich mosaic: it can "reveal a person's religion, political associations, use of a telephone-sex hotline, contemplation of suicide, addiction to gambling or drugs, experience with rape, grappling with sexuality, or support for particular political causes." Decl. of Edward Felten, Professor of Computer Science and Public Affairs, Princeton University, ¶ 42 (ECF No. 27). But that is at least three inflections from the Government's bulk telephony metadata collection. First, without additional legal justification—subject to rigorous minimization procedures—the NSA cannot even query the telephony metadata database. Second, when it makes a query, it only learns the telephony metadata of the telephone numbers within three "hops" of the "seed."

Third, without resort to additional techniques, the Government does not know who any of the telephone numbers belong to. In other words, all the Government sees is that telephone number A called telephone number B. It does not know who subscribes to telephone numbers A or B. Further, the Government repudiates any notion that it conducts the type of data mining the ACLU warns about in its parade of horribles.[17]

The ACLU also argues that "[t]here are a number of ways in which the Government could perform three-hop analysis without first building its own database of every American's call records." Supp. Decl. of Edward Felten, ¶ 6 (ECF No. 68-1). That has no traction. At bottom, it is little more than an assertion that less intrusive means to collect and analyze telephony metadata could be employed. But, the Supreme Court has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment." City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2632 (2010) (citing Vernonia School Dist. 47J v. Acton, 115 S. Ct. 2386, 2396 (1995)). That judicial-Monday-morning-quarterbacking "could raise insuperable barriers to the exercise of virtually all search-and-seizure powers" because judges engaging in after-the-fact evaluations of government conduct "can almost always imagine some alternative means by which the objectives might have been

---

[17] General Alexander's testimony on this point is crystal clear:

> [I]n the open press there's this discussion about pattern analysis—[that the Government is] out there doing pattern analysis on this. That is absolutely incorrect. We are not authorized to go into the data, nor are we data mining, or doing anything with the data other than those queries that we discuss, period. We're not authorized to do it. We aren't doing it. There are no automated processes running in the background pulling together data trying to figure out networks. . . . The only time you can do pattern analysis is, once you start the query on that query and where you go forward.

Alexander Testimony at 66.

accomplished." Quon, 130 S. Ct. at 2632 (internal quotation marks and citations omitted).

The ACLU's pleading reveals a fundamental misapprehension about ownership of telephony metadata. In its motion for a preliminary injunction, the ACLU seeks to: (1) bar the Government from collecting "Plaintiffs' call records" under the bulk telephony metadata collection program; (2) quarantine "all of Plaintiffs' call records" already collected under the bulk telephony metadata collection program; and (3) prohibit the Government from querying metadata obtained through the bulk telephony metadata collection program using any phone number or other identifier associated with Plaintiffs. Pls. Mot. at 2.

First, the business records created by Verizon are not "Plaintiffs' call records." Those records are created and maintained by the telecommunications provider , not the ACLU. Under the Constitution, that distinction is critical because when a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information. See Smith, 422 U.S. at 742. Second, the Government's subsequent querying of the telephony metadata does not implicate the Fourth Amendment—anymore than a law enforcement officer's query of the FBI's fingerprint or DNA databases to identify someone. See Maryland v. King, 133 S. Ct. 1958, 1963-64 (2013). In the context of DNA querying, any match is of the DNA profile—and like telephony metadata additional investigative step are required to link that DNA profile to an individual.

The collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search. Cf. United States v. Dionisio, 410 U.S. 1, 13 (1973) (Where single grand jury subpoena did not constitute unreasonable seizure, it could not be "rendered unreasonable by the fact that may others were

subjected to the same compulsion"); In re Grand Jury Proceedings: Subpoena Duces Tecum, 827 F.2d at 305 ("[T]he fourth amendment does not necessarily prohibit the grand jury from engaging in a 'dragnet' operation.") (citation omitted).

The ACLU's reliance on the concurring opinions in Jones is misplaced. In Jones, the police attached a GPS tracking device to the undercarriage of a vehicle without a warrant and tracked the vehicle's location for the next four weeks. 132 S. Ct. at 948. The majority held that a "search" occurred because by placing the GPS device on the vehicle, "[t]he Government physically occupied private property for the purpose of obtaining information. . . . [S]uch a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." Jones, 132 S. Ct. at 949 (citation omitted). In two separate concurring opinions, five justices appeared to be grappling with how the Fourth Amendment applies to technological advances. Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring); Jones, 132 S. Ct. at 964 (Alito, J., concurring).

But the Supreme Court did not overrule Smith. And the Supreme Court has instructed lower courts not to predict whether it would overrule a precedent even if its reasoning has been supplanted by later cases. "[T]he Court of Appeals should . . . leav[e] to th[e Supreme] Court the prerogative of overruling its own decisions." Agostini v. Felton, 521 U.S. 203, 237 (1997) (quoting Rodriguez de Quijas v. Shearson/Am. Express, Inc., 490 U.S. 477, 484 (1989)). Clear precedent applies because Smith held that a subscriber has no legitimate expectation of privacy in telephony metadata created by third parties. See Smith, 442 U.S. at 744–45. Inferior courts are bound by that precedent.

Some ponder the ubiquity of cellular telephones and how subscribers' relationships with their telephones have evolved since Smith. While people may "have an entirely different relationship with telephones than they did thirty-four years ago," Klayman, 2013 WL 6571596, at *21, this Court observes that their relationship with their telecommunications providers has not changed and is just as frustrating. Telephones have far more versatility now than when Smith was decided, but this case only concerns their use as telephones. The fact that there are more calls placed does not undermine the Supreme Court's finding that a person has no subjective expectation of privacy in telephony metadata. See Smith, 442 U.S. at 745. ("The fortuity of whether or not the [tele]phone company in fact elects to make a quasi-permanent record of a particular number dialed does not . . . make any constitutional difference. Regardless of the [tele]phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record.") Importantly, "what metadata is has not changed over time," and "[a]s in Smith, the types of information at issue in this case are relatively limited: [tele]phone numbers dialed, date, time, and the like." Klayman, 2013 WL 6571596, at *21 (emphasis in original). Because Smith controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment.

B. First Amendment

"[I]mplicit in the right to engage in activities protected by the First Amendment [is] a corresponding right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends." Roberts v. U.S. Jaycees, 468 U.S. 609, 622 (1984). Pervasive Government surveillance implicates not only the Fourth Amendment but also the First Amendment:

> National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power. History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies.

Keith, 407 U.S. at 313–14 (internal quotation marks and citation omitted).

The ACLU alleges that "[t]he fact that the government is collecting this information is likely to have a chilling effect on people who would otherwise contact Plaintiffs." Compl. ¶ 35. Significant impairments of first amendment rights "must withstand exacting scrutiny." United States v. Alvarez, 132 S. Ct. 2537, 2548 (2012); see also Nat'l Commodity & Barter Ass'n v. Archer, 31 F.3d 1521, 1531 n.4 (10th Cir. 1994); In re Grand Jury Proceedings, 776 F.2d 1099, 1102–03 (2d Cir. 1985). The Government contends, however, that "surveillance consistent with Fourth Amendment protections . . . does not violate First Amendment rights, even though it may be directed at communicative or associative activities." Gordon v. Warren Consol. Bd. of Educ., 706 F.2d 778, 781 n.3 (6th Cir. 1983).

The Government's argument is well-supported. See, e.g., United States v. Mayer, 503 F.3d 740, 747–48 (9th Cir. 2007) (noting that "Fourth Amendment provides the relevant benchmark" for a challenge to a criminal investigation on First Amendment grounds); Anderson v. Davila, 125 F.3d 148, 160 (3d Cir. 1997) ("Government's surveillance of individuals in public places does not, by itself, implicate the Constitution" absent evidence of retaliatory conduct for protected activities); Phila. Yearly Meeting of Religious Soc. of Friends v. Tate, 519 F.2d 1335, 1337–38 (3d Cir. 1975) (upholding police surveillance activities limited to data gathering at

public meetings); United States v. Oaks, 527 F.2d 937, 941 (9th Cir. 1975) (upholding surveillance by undercover agent of public meeting of tax rebellion group); Lustiger v. United States, 386 F.2d 132, 139 (9th Cir. 1967) (holding that "the Fourth Amendment does not preclude postal inspectors from copying information contained on the outside of sealed envelopes in the mail"); Cohen v. United States, 378 F.2d 751, 760 (9th Cir. 1967) (rejecting First Amendment challenge to the "mail cover" practice). And this consideration is built in to any section 215 application. See 50 U.S.C. § 1861 (requiring that the investigation not be conducted "solely upon the basis of activities protected by the [F]irst [A]mendment").

Here, it is unnecessary to decide whether there could be a First Amendment violation in the absence of a Fourth Amendment violation because Amnesty International compels the conclusion that the bulk metadata collection does not burden First Amendment rights substantially. Cf. 133 S. Ct. at 1152. "[D]istinguishing between incidental and substantial burdens under the First Amendment requires a different analysis, applying different legal standards, than distinguishing what is and is not routine in the Fourth Amendment . . . context." Tabbaa v. Chertoff, 509 F.3d 89, 102 n.4 (2d Cir. 2007). There must be "a direct and substantial" or "significant" burden on associational rights in order for it to qualify as "substantial." Tabbaa, 509 F.3d at 101. "Mere incidental burdens on the right to associate do not violate the First Amendment." Tabbaa, 509 F.3d at 101.

Any alleged chilling effect here arises from the ACLU's speculative fear that the Government will review telephony metadata related to the ACLU's telephone calls. For telephony metadata to be "used to identify those who contact Plaintiffs for legal assistance or to report human-rights or civil-liberties violations," Compl. ¶ 35, it must actually be reviewed and

the identities of the telephone subscribers determined. Fear that telephony metadata relating to the ACLU will be queried or reviewed or further investigated "relies on a highly attenuated chain of possibilities." Amnesty Int'l, 133 S. Ct. at 1148. "[S]uch a fear is insufficient to create standing," Amnesty Int'l, 133 S. Ct. at 1152. Neither can it establish a violation of an individual's First Amendment rights.

IV. Remaining Preliminary Injunction Considerations

For the reasons above, the ACLU has failed to state a claim and its case must be dismissed. But even if it could show a likelihood of success on the merits, a preliminary injunction would be inappropriate. "A preliminary injunction is an 'extraordinary and drastic remedy.' It should never be awarded as of right." Munaf, 553 U.S. at 676 (quoting Yakus v. United States, 321 U.S. 414, 440 (1944)). As discussed above, "[a] plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." Winter, 555 U.S. at 20.

Here, the balance of the equities and the public interest tilt firmly in favor of the Government's position. "Everyone agrees that the Government's interest in combating terrorism is an urgent objective of the highest order." Holder v. Humanitarian Law Project, 130 S. Ct. 2705, 2724 (2010); see also Haig v. Agee, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.") (internal quotation marks omitted); In re Directives [REDACTED] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) ("[T]he relevant government interest—the interest in national security—is of the highest order of

magnitude.").

The Constitution vests the President with Executive Power. U.S. Const. Art. II. That power reaches its zenith when wielded to protect national security. Cf. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring) ("When the President acts pursuant to an express or implied authorization from Congress," his actions are "supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion . . . rest[s] heavily upon any who might attack it." (internal quotations omitted)). And courts must pay proper deference to the Executive in assessing the threats that face the nation. Boumediene v. Bush, 553 U.S. 723, 797 (2008) ("[M]ost federal judges [do not] begin the day with briefings that may describe new and serious threats to our Nation and its people."). Any injunction dismantling the section 215 telephony metadata collection program "would cause an increased risk to national security and the safety of the American public." Shea Decl. ¶ 63. The "unique capabilities" of the telephony metadata collection program "could not be completely replicated by other means." Shea Decl. ¶ 63.

The effectiveness of bulk telephony metadata collection cannot be seriously disputed. Offering examples is a dangerous stratagem for the Government because it discloses means and methods of intelligence gathering. Such disclosures can only educate America's enemies. Nevertheless, the Government has acknowledged several successes in Congressional testimony and in declarations that are part of the record in this case. In this Court's view, they offer ample justification:

- In September 2009, NSA discovered that an al-Qaeda-associated terrorist in Pakistan was in contact with an unknown person in the United States about efforts to perfect a recipe for explosives. NSA immediately notified the FBI, which investigated and identified the al-Qaeda contact as

> Colorado-based Najibullah Zazi. The NSA and FBI worked together to identify other terrorist links. The FBI executed search warrants and found bomb-making components in backpacks. Zazi confessed to conspiring to bomb the New York subway system. Through a section 215 order, NSA was able to provide a previously unknown number of one of the co-conspirators—Adis Medunjanin.
>
> - In January 2009, while monitoring an extremist in Yemen with ties to al-Qaeda, the NSA discovered a connection with Khalid Oazzani in Kansas City. NSA immediately notified the FBI, which discovered a nascent plot to attack the New York Stock Exchange. Using a section 215 order, NSA queried telephony metadata to identify potential connections. Three defendants were convicted of terrorism offenses.
>
> - In October 2009, while monitoring an al-Qaeda affiliated terrorist, the NSA discovered that David Headley was working on a plot to bomb a Danish newspaper office that had published cartoons depicting the Prophet Mohammed. He later confessed to personally conducting surveillance of the Danish newspaper office. He was also charged with supporting terrorism based on his involvement in the planning and reconnaissance for the 2008 hotel attack in Mumbai. Information obtained through section 215 orders was utilized in tandem with the FBI to establish Headley's foreign ties and put them in context with U.S. based planning efforts.

Holley Decl. ¶ 24–26; Testimony before the House Permanent Select Committee on Intelligence, dated June 18, 2013, FBI Deputy Director Sean Joyce, at 12–13 (ECF No. 33-13) [hereinafter "Joyce Testimony"].

Bulk telephony metadata collection is one tool used to thwart potential terrorist attacks. Deputy Director Joyce explained:

> Our mission is to stop terrorism, to prevent it. Not after the fact, to prevent it before it happens in the United States. And I can tell you every tool is essential and vital. And the tools as I outlined to you and their uses today have been valuable to stopping some of those plots. You ask, 'How can you put the value on an American life?' And I can tell you, its priceless.

Joyce Testimony at 52.

Of course, the considerations weighing in favor of the ACLU's position are far

from trivial. The need for the telephony metadata collection program "does not make the employment by Government of electronic surveillance a welcome development—even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens." Keith, 407 U.S. at 312. Just as the Constitution gives the Executive the duty to protect the nation, citizens' right to privacy is enshrined in the Bill of Rights.

Fifteen different FISC judges have found the metadata collection program lawful a total of thirty-five times since May 2006. See Holley Decl. ¶¶ 6, 11; In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From [REDACTED], No. BR 13-158 (F.I.S.C. Oct. 11, 2013). The Government argues that "Plaintiffs are asking this Court to conclude that the FISC exceeded its authority when it authorized the NSA's bulk collection of telephony metadata, and that this Court (without the benefit of the classified applications and information available to the FISC) should substitute its judgment for the decisions that the FISC reached [35] times." Gov't Prelim. Inj. Opp. Br. at 16–17 (ECF No. 61) (internal citation omitted).

This Court is bound only by the decisions of the Second Circuit and the Supreme Court. The decisions of other district courts are often persuasive authority. The two declassified FISC decisions authorizing bulk metadata collection do not discuss several of the ACLU's arguments. They were issued on the basis of ex parte applications by the Government without the benefit of the excellent briefing submitted to this Court by the Government, the ACLU, and amici curiae.

There is no question that judges operate best in an adversarial system. "The value

of a judicial proceeding . . . is substantially diluted where the process is ex parte, because the Court does not have available the fundamental instrument for judicial judgment: an adversary proceeding in which both parties may participate." Carroll v. President & Comm'rs of Princess Anne, 393 U.S. 175, 183 (1968). At its inception, FISC judges were called on to review warrant applications, a familiar role and one well-suited for a judge to protect the rights of an individual in his absence. The FISC's role has expanded greatly since its creation in 1978.

As FISA has evolved and Congress has loosened its individual suspicion requirements, the FISC has been tasked with delineating the limits of the Government's surveillance power, issuing secret decision without the benefit of the adversarial process. Its ex parte procedures are necessary to retain secrecy but are not ideal for interpreting statutes. This case shows how FISC decisions may affect every American—and perhaps, their interests should have a voice in the FISC.

CONCLUSION

The right to be free from searches and seizures is fundamental, but not absolute. As Justice Jackson famously observed: "the Bill of Rights is not a suicide-pact." Terminiello v. City of Chicago, 337 U.S. 1 (1949). Whether the Fourth Amendment protects bulk telephony metadata is ultimately a question of reasonableness. Missouri v. McNeely, 133 S. Ct. 1552, 1569–70 (2013) ("[T]he ultimate touchstone of the Fourth Amendment is reasonableness."). Every day, people voluntarily surrender personal and seemingly-private information to trans-national corporations, which exploit that data for profit. Few think twice about it, even though it is far more intrusive than bulk telephony metadata collection.

There is no evidence that the Government has used any of the bulk telephony

metadata it collected for any purpose other than investigating and disrupting terrorist attacks. While there have been unintentional violations of guidelines, those appear to stem from human error and the incredibly complex computer programs that support this vital tool. And once detected, those violations were self-reported and stopped. The bulk telephony metadata collection program is subject to executive and congressional oversight, as well as continual monitoring by a dedicated group of judges who serve on the Foreign Intelligence Surveillance Court.

No doubt, the bulk telephony metadata collection program vacuums up information about virtually every telephone call to, from, or within the United States. That is by design, as it allows the NSA to detect relationships so attenuated and ephemeral they would otherwise escape notice. As the September 11th attacks demonstrate, the cost of missing such a thread can be horrific. Technology allowed al-Qaeda to operate decentralized and plot international terrorist attacks remotely. The bulk telephony metadata collection program represents the Government's counter-punch: connecting fragmented and fleeting communications to re-construct and eliminate al-Qaeda's terror network.

"Liberty and security can be reconciled; and in our system they are reconciled within the framework of the law." Boumediene, 553 U.S. at 798. The success of one helps protect the other. Like the 9/11 Commission observed: The choice between liberty and security is a false one, as nothing is more apt to imperil civil liberties than the success of a terrorist attack on American soil. The 9/11 Commission Report, at 395. A court's solemn duty is "to reject as false, claims in the name of civil liberty which, if granted, would paralyze or impair authority to defend [the] existence of our society, and to reject as false, claims in the name of security which

would undermine our freedoms and open the way to oppression. American Comm'cns Ass'n, C.I.O. v. Douds, 339 U.S. 382, 445 (1950) (Jackson, J., concurring in part and dissenting in part).

For all of these reasons, the NSA's bulk telephony metadata collection program is lawful. Accordingly, the Government's motion to dismiss the complaint is granted and the ACLU's motion for a preliminary injunction is denied. The Clerk of Court is directed to terminate the motions pending at ECF Nos. 25 and 32 and to mark this case closed.

Dated: December 27, 2013
New York, New York

SO ORDERED:

WILLIAM H. PAULEY III
U.S.D.J.

Counsel of Record:
Jameel Jaffer, Esq.
Alex A. Abdo, Esq.
Brett M. Kaufman, Esq.
Patrick C. Toomey, Esq.
Catherine N. Crump, Esq.
American Civil Liberties Union
125 Broad Street
New York, NY 10004

Arthur N. Eisenberg, Esq.
Christopher T. Dunn, Esq.
New York Civil Liberties Union
125 Broad Street, 17th Floor
New York, NY 10004

Laura Donohue, Esq.
Georgetown Law
5417 Duvall Drive
Bethesda, MD 20816
Counsel for Plaintiffs

David S. Jones, Esq.
Tara M. La Morte, Esq.
Christopher B. Harwood, Esq.
John D. Clopper, Esq.
U.S. Attorney's Office, S.D.N.Y.
86 Chambers Street
New York, NY 10007
Counsel for Defendants

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

AMERICAN CIVIL LIBERTIES UNION, et al.,

Plaintiffs,

-against-

JAMES R. CLAPPER, et al.,

Defendants.

----------X

13 **CIVIL** 3994 (WHP)

JUDGMENT

The ACLU having moved for a preliminary injunction and the Government having moved to dismiss the complaint, and the matter having come before the Honorable William H. Pauley III, United States District Judge, and the Court, on December 27, 2013, having rendered its Memorandum and Order finding the NSA's bulk telephony metadata collection program is lawful, accordingly, granting the Government's motion to dismiss the complaint, and denying the ACLU's motion for a preliminary injunction, it is,

ORDERED, ADJUDGED AND DECREED: That for the reasons stated in the Court's Memorandum and Order dated December 27, 2013, the Court finds the NSA's bulk telephony metadata collection program is lawful; accordingly, the Government's motion to dismiss the complaint is granted and the ACLU's motion for a preliminary injunction is denied and the case is closed.

Dated: New York, New York
December 27, 2013

RUBY J. KRAJICK

Clerk of Court

BY:

Deputy Clerk

THIS DOCUMENT WAS ENTERED
ON THE DOCKET ON _____

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 ROBERT S. MUELLER III, in his official capacity as Director of the Federal Bureau of Investigation, *Defendants*.	No. 13-cv-03994 (WHP) **ECF CASE**

NOTICE OF APPEAL

NOTICE IS HEREBY GIVEN that the American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, and New York Civil Liberties Union Foundation hereby appeal to the United States Court of Appeals for the Second Circuit from the Judgment entered in this action on December 27, 2013 [Docket #77], granting Defendants' motion to dismiss Plaintiffs' complaint and denying Plaintiffs' motion for a preliminary injunction.

Respectfully submitted,

/s/ Jameel Jaffer

Jameel Jaffer (JJ-4653)
Alex Abdo (AA-0527)
Patrick Toomey (PT-1452)
Brett Max Kaufman (BK-2827)
Catherine Crump (CC-4067)
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
jjaffer@aclu.org

Christopher T. Dunn (CD-3991)
Arthur N. Eisenberg (AE-2012)
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004
Phone: (212) 607-3300
Fax: (212) 607-3318
aeisenberg@nyclu.org

January 2, 2014