EXHIBIT 4

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LARRY KLAYMAN, *et al.*, Plaintiffs, v. BARACK OBAMA, President of the United States, *et al.*, Defendants.	Civil Action No. 13-cv-0851 (RJL)

DECLARATION OF MAJOR GENERAL GREGG C. POTTER,
SIGNALS INTELLIGENCE DEPUTY DIRECTOR,
NATIONAL SECURITY AGENCY

I, Gregg C. Potter, do hereby state and declare as follows:

1. I am the Deputy 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 ("SIGINT") activities, sources, and methods against unauthorized disclosures. Under Executive Order ("E.O.") 12333, 46 Fed. Reg. 59941 (1981), as amended on January 23, 2003, 68 Fed. Reg. 4075 (2003), 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 SIGINT information for the foreign intelligence purposes of the United States. I have been designated an original TOP SECRET classification authority under E.O. 13526, 75 Fed. Reg. 707 (Jan. 5, 2010).

2. I have read the declarations of Teresa H. Shea, dated October 1, 2013 and May 1, 2014, which were submitted in the above-captioned matter on November 12, 2013 and May 9, 2014, respectively. Those declarations provided a detailed overview of the NSA's bulk

telephony metadata program carried out pursuant to orders of the Foreign Intelligence Surveillance Court ("FISC") under Section 215 of the USA-PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (the "Program")—including changes that were announced to the Program by the President in January 2014—and discussed minimization procedures, oversight of the Program, the benefits that the Program provides for the protection of the United States against potential terrorist threats, and the burden of complying with the preliminary injunctive relief that had been requested by plaintiffs at the time.

3. I submit this declaration to discuss changes to the Program since those declarations were made, including Congress's passage of the USA FREEDOM Act, the imminent termination of the Program on November 28, 2015, and the transition to a new targeted metadata collection program under the USA FREEDOM Act. I also discuss the Government's plans for temporary retention (subject to FISC approval) of the metadata collected under the Program after transition to the new targeted metadata collection program, and the burdens and potential consequences of the injunctive relief currently sought by plaintiffs. I also address certain speculation concerning the scope of the Program. My statements herein are based upon my personal knowledge of SIGINT collection and NSA operations, and information made available to me in my capacity as SID Deputy Director.

EVOLUTION OF THE PROGRAM

4. The Declaration of Teresa H. Shea, dated October 1, 2013, provides a detailed and accurate description of the Program as it existed at the time. Since that declaration, and since this Court's initial decision on December 16, 2013, to grant a preliminary injunction in this case, there have been a number of significant changes to the Program, affecting the way it works and when it will end.

5. On January 17, 2014, following a review of the nation's SIGINT programs, the President announced a series of reforms designed to preserve the Intelligence Community's capabilities to detect and prevent threats by foreign terrorist organizations, while enhancing protections for individual privacy as intelligence capabilities developed to meet the threat of international terrorism continue to advance. A transcript of the President's remarks is available at http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

6. Regarding the Program, the President directed: (1) that the Government work with the FISC to require advance findings by FISC judges of "reasonable, articulable suspicion" that selectors (such as telephone numbers) used to query the metadata are associated with terrorist organizations (except in emergency situations, in which FISC approval is to be sought retrospectively); and (2) that query results available to NSA analysts be limited to metadata within two "hops" (degrees of contact) of suspected terrorist selectors, not three as previously allowed.

7. The Government took immediate steps to put these two changes into effect, including filing a motion with the FISC to amend its January 3, 2014 Primary Order approving the Program. The Government's motion proposed that the order be changed so that (1) except in cases of emergency, the Government is required to obtain advance permission from the FISC to use a proposed selector as a "seed" to query the telephone metadata, predicated on a finding by the FISC that the selector to be used satisfies the "reasonable, articulable suspicion" standard, and (2) each metadata query be limited to two "hops" rather than the three "hops" that previously had been permitted. On February 5, 2014, the FISC granted the Government's motion to implement these two changes to the Program. *In re Application of the FBI for an Order*

Requiring the Production of Tangible Things from [Redacted], Dkt. No. BR 14-01 (F.I.S.C. Feb 5, 2014) (publicly released, unclassified version). These changes remain in effect to this day. Attached as Exhibit A is a true and correct copy (in declassified form) of the most recent FISC Primary Order authorizing the Program, dated August 27, 2015 ("Aug. 27 Primary Order"), which reflects these changes to the Program. Including this most recent order, at least 19 different FISC judges have entered a total of 43 orders authorizing NSA's bulk collection of telephony metadata under Section 215.

8. The President also ordered the Intelligence Community and the Attorney General to develop options for a new approach that would match the Program's capabilities without the Government continuing to hold the bulk telephony metadata. The Intelligence Community and the Attorney General immediately began developing options to present to the President. On March 27, 2014, after having considered those options, the President announced that he would seek legislation to replace the Program. *See* http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program. The President stated that his goal was to "establish a mechanism to preserve the capabilities we need without the Government holding this bulk metadata" to "give the public greater confidence that their privacy is appropriately protected," while maintaining the intelligence tools needed "to keep us safe."

9. The President's proposal for the new program focused on the concept that the metadata would remain in the hands of telecommunications companies instead of the Government collecting it in bulk. The President stated that "legislation will be needed to permit the Government to obtain information with the speed and in the manner that will be required to make this approach workable." Under such legislation, the Government would be authorized to obtain telephony metadata from the companies pursuant to targeted orders from the FISC. The

President explained that, in the meantime, the Government would seek reauthorization of the existing program from the FISC, incorporating the two modifications already approved by the FISC in February 2014.

THE USA FREEDOM ACT

10. On June 2, 2015, Congress passed, and the President signed, the USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268. This legislation was the culmination of the President's proposal for a new targeted telephony metadata program to replace the Program. The new law reauthorized Section 215 but, beginning on November 29, 2015, prohibits the Government from obtaining telephony metadata in bulk under Section 215, bringing an end to the Program. In its place, Congress authorized a new mechanism providing for targeted production of call detail records by the providers.

11. The USA FREEDOM Act gives the Government new authorities needed to enable it to obtain targeted productions of metadata from the providers with the speed and in the manner required to make this new approach possible. For instance, Section 101(b) of the USA FREEDOM Act, which becomes effective November 29, 2015, will require providers who receive orders under the amended Section 215 to: (1) produce records "in a form that will be useful to the Government" and (2) "furnish the Government forthwith all information, facilities, or technical assistance necessary to accomplish the production in such a manner as will protect the secrecy of the production and produce a minimum of interference with the services that such person is providing to each subject of the production." These new authorities are critical to ensuring that providers develop the necessary technical infrastructure to make prompt production of call detail records in response to targeted requests made pursuant to orders under the USA FREEDOM Act (known as the "query-at-the-provider" model).

12. The USA FREEDOM Act provides for a 180-day transition period before certain amendments to Section 215, including its prohibition on bulk collection of telephony metadata, become effective. As NSA Director Admiral Michael S. Rogers noted in a letter to Senate Leadership on May 20, 2015, the transition period allows the NSA to "work with the companies that are expected to be subject to Orders under the law by providing them the technical details, guidance, and compensation to create a fully operational query-at-the-provider model." Letter from ADM Michael S. Rogers to Senators McConnell and Reid (May 20, 2015) (a true and correct copy of this letter is attached as Exhibit B). The NSA began that process upon passage of the USA FREEDOM Act, and is working diligently to ensure that the new querying model is brought on-line by the end of the 180-day transition period.

13. However, the new querying model is not yet operational, though NSA expects it to be operational by the end of the 180-day transition period. Moreover, the Government's new authorities to compel technical assistance from providers and the production of records "in a form that will be useful to the Government" do not become effective under the law until November 29, 2015. Accordingly, the NSA does not expect that the query-at-the-provider model will be operational until November 29, 2015.

14. After the reauthorization of Section 215 by the USA FREEDOM Act, the Government applied to the FISC for authorization to resume the Program during the 180-day transition period. The FISC granted the Government's application on June 29, 2015, and renewed that authorization on August 27, 2015. Under the most recent FISC authorization, the Government's ability to collect telephony metadata in bulk expires on November 28, 2015, in synch with the effective date of the USA FREEDOM Act's prohibition on bulk collection.

POST-TRANSITION HANDLING OF METADATA COLLECTED UNDER THE PROGRAM

15. The most recent FISC Primary Order does not authorize the retention or use of metadata collected under the Program beyond November 28, 2015. The Government has requested authority from the FISC to retain the historical bulk metadata for purposes of (1) any applicable preservation obligations in still-pending litigation involving the Program, and (2) allowing technical personnel continued access to the historical bulk metadata until February 29, 2016, solely to verify the completeness and accuracy of records produced under the new targeted production mechanism authorized by the USA FREEDOM Act. The FISC has taken these requests under advisement. As disclosed in an official statement by the Office of the Director of National Intelligence on July 27, 2015, the NSA has determined that, even if the FISC approves retention of the historical bulk metadata for the above-described purposes, analytic access to the historical bulk metadata collected under the Program will cease after November 28, 2015. Following the expiration of the current Primary Order on that date, the Government will no longer have FISC approval to conduct analytic queries of the retained data for purposes of acquiring foreign-intelligence information.

16. Notwithstanding the forthcoming termination of the Program, there remain a number of civil actions (including this case) involving legal challenges to the Program, and the NSA remains subject to legal obligations regarding the preservation of potentially relevant evidence. In light of these preservation obligations, the NSA has decided to preserve (subject to FISC approval) historical metadata collected under the Program until civil litigation regarding the Program is resolved, or the courts in these cases relieve the NSA of any applicable obligations to preserve such data.

17. Historical bulk metadata preserved beyond November 28, 2015 will only be used or accessed, as approved by the FISC: (1) to satisfy legal obligations in connection with civil litigation and/or (2) to permit technical personnel, until February 29, 2016, to verify the completeness and accuracy of records produced under the new targeted production mechanism authorized by the USA FREEDOM Act.

SCOPE OF THE SECTION 215 BULK TELEPHONY METADATA PROGRAM

18. Although plaintiffs and other members of the public have speculated that the NSA, under the Program, acquires metadata relating to all telephone calls to, from, or within the United States, that is not the case. The Government has acknowledged that the Program is broad in scope and involves the collection and aggregation of a large volume of data from multiple providers, but the Program has never captured information on all (or virtually all) calls made and/or received in the United States.

19. While the Government has also acknowledged that one provider, Verizon Business Network Services, was the recipient of a now-expired April 25, 2013 Secondary Order from the FISC, the identities of the carriers participating in the Program (either now, or at any other time) otherwise remain classified.

THE EFFECT OF COMPLIANCE WITH A POTENTIAL PRELIMINARY INJUNCTION

20. I understand that plaintiffs seek or have sought a preliminary injunction that would potentially prohibit the NSA from taking various actions, including (1) collecting metadata associated with plaintiffs' telephone calls as part of the Program, and (2) conducting analytic queries of or accessing for analytic purposes any metadata associated with plaintiffs' calls that may already have been collected as part of the Program. Below I address the burden and impact of complying with such prohibitions. This assessment is informed by the

Government's extensive inter-agency discussions and planning regarding the steps required to comply with the Court's December 16, 2013 injunction, should that injunction have been upheld on appeal.

21. I understand that plaintiffs have requested as part of their motion that NSA not destroy any metadata records relating to plaintiffs' calls until the conclusion of the case. Accordingly, I will not address in this declaration the burden and impact of destroying metadata associated with particular plaintiffs' calls other than to state that such relief (particularly to the extent it would involve destruction of records contained on system backup tapes) would present extraordinarily burdensome technical and logistical hurdles that could be overcome only at great expense and commitment of scarce technical and personnel resources. These burdens can be described in greater detail if necessary at a later date.

22. To comply with a Court order to cease either collection or queries of metadata pertaining to plaintiffs' telephone calls (or both), the NSA first would have to be provided with the telephone numbers or calling card numbers used by plaintiffs. Call-detail records collected under the Program include the dialing and receiving telephone numbers (among other data), but do not include the identities of the parties to the calls or even of the subscribers to whom the numbers are assigned. *See* Aug. 27, 2015 Primary Order at 3, n.1. Accordingly, compliance with any injunction concerning the telephony metadata associated with plaintiffs would first require that plaintiffs: (1) identify all telephone numbers and calling card numbers used by them during the period from March 12, 2009 to present; (2) identify the time frames during which each telephone number and calling card number was used by each plaintiff within the relevant period; and (3) provide the Government with timely updates to this information when new numbers are used or when plaintiffs cease to use certain numbers. Until such information is

provided to the Government, the NSA could not comply with any injunction barring collection or queries of telephony metadata associated with plaintiffs' calls. It is not possible for the NSA to estimate how long it would take to obtain this information because that is a matter within plaintiffs' control, not the NSA's. If the NSA were required to comply immediately with an injunction prohibiting the collection, query, or analytic use of telephony metadata associated with plaintiffs' calls, without plaintiffs having first provided this information, it would require termination of all collection and queries of data already collected under the Program.

23. Additionally, because the NSA does not acquire subscriber or customer names through the Program, *see* Aug. 27, 2015 Primary Order at 3 n.1, it is not currently known whether metadata about the plaintiffs' telephone calls are (or have been) acquired as part of the Program. Whether such information is being (or has been) acquired through the Program can be determined only after the NSA's receipt of the plaintiffs' phone numbers as described in paragraph 22, by querying the metadata for those selection terms. The FISC's August 27, 2015 Order, however, currently restricts searches of the metadata to queries undertaken for purposes of obtaining foreign intelligence information (using FISC-approved selection terms that satisfy the reasonable articulable suspicion standard, except in emergency situations) and for limited technical purposes, for example, to make the data usable for intelligence analysis. *Id.* at 5–9. That Order provides: "[t]he Government is . . . prohibited from accessing BR metadata for any purpose except as described [there]in." *Id.* at 4. Thus, if this Court were to issue an injunction requiring the NSA to take action with respect to any metadata about the plaintiffs' telephone calls, the NSA would need to engage promptly with the FISC as to queries of the database for these purposes and to obtain a modification of the FISC's Orders if it did not view such queries as currently authorized. The NSA cannot estimate the amount of time necessary to complete this

process, however, since the timeframe would depend upon the FISC's response to the Government's proposal, including whether it would require the Government to seek a modification of its Orders in order to perform such queries. Moreover, the NSA cannot know in advance how the FISC would respond to such a request if made. If the NSA were required to comply immediately with an injunction prohibiting the collection, querying, or analytic use of telephony metadata associated with plaintiffs' calls, without having first engaged with the FISC and, if deemed necessary, having obtained a modification of its Orders to permit the NSA to query the metadata for the plaintiffs' telephone numbers, it would require termination of all collection and queries of data already collected under the Program.

24. The discussion below regarding the effect of compliance with a potential preliminary injunction assumes that (1) plaintiffs provide their telephone numbers to the NSA; (2) the NSA's querying of the metadata for those selection terms is permitted by FISC Order; and (3) those queries indicate that metadata about the plaintiffs' telephone calls is or was acquired as part of the Program.[1]

25. Even if the NSA were provided with the necessary information regarding plaintiffs' telephone numbers and the queries described above are permitted by FISC Order, immediate compliance with an order barring collection of metadata associated with plaintiffs' telephone calls could still require termination of all collection under the Program. To prevent the

[1] If such queries instead indicate that metadata about plaintiffs' calls was not and is not acquired as part of the Program, the burdens of compliance would be reduced, but not eliminated. NSA would still be required to ensure that metadata about plaintiffs' calls is not ingested in any future collection under the Program, which, as described in ¶ 25, creates a significant burden and could require a shutdown of collection under the Program. NSA would not be able to publicly state whether or not metadata associated with plaintiffs' calls was identified by any search because doing so would reveal information that is currently and properly classified. The Government would need to inform the Court of the results of its search *in camera* and *ex parte*.

collection under the Program of call detail records containing specific identifiers, participating providers would have to develop the capability to filter out records containing specific identifiers from their bulk productions before they were transmitted to the NSA. It is not possible for the NSA to estimate how long it would take providers to develop this capability, or at what cost. If the NSA were required to comply immediately with an injunction prohibiting the receipt of telephony metadata associated with plaintiffs' calls, the NSA would have to shut down all collection under the Program.

26. Furthermore, even if an injunction barring collection of records associated with plaintiffs' calls permitted the NSA to filter out the records after they were received from a provider, the NSA still would need to develop a process to delete or segregate upon ingestion into its databases any call detail records containing the selectors identified by plaintiffs. NSA technical personnel estimate that it would take two full-time employees approximately two months to design, code, and test such a process.[2] Because the Program is scheduled to be shut down on November 28, 2015, it is unlikely that this process would be operational before the termination of the Program. If the NSA were required to comply immediately with an injunction to delete or segregate records associated with plaintiffs' calls as soon as they are ingested into its databases, it would require a complete shutdown of collection under the Program.

27. With respect to a requirement that the NSA cease analytic access to any records about plaintiffs' calls that may already have been collected under the Program, NSA has developed a process that can be used to prevent analytic access to metadata containing specified

[2] Adding other personnel to the project would have only a marginal effect on shortening the time needed to complete this process because: (1) a limited number of personnel have the training and knowledge of affected systems to perform this work; and (2) the work for such a project cannot easily be partitioned into discrete tasks without requiring additional time for communication and coordination.

identifiers. This capability prevents the use of particular identifiers to conduct queries, and prevents analysts from accessing records containing those identifiers even if responsive to queries using different identifiers. NSA technical personnel estimate that eliminating analytic access to metadata associated with plaintiffs' calls could be completed within approximately 2 weeks after the receipt of plaintiffs' telephone numbers and the time-frames during which they were used (as discussed in paragraph 22, above). If the NSA were required to comply immediately with an injunction prohibiting analytic access to or use of telephony metadata associated with plaintiffs' calls, all queries of the metadata collected under the Program would have to terminate until such time as the above-described process can be completed.

THE EFFECT OF DISRUPTION OF THE SECTION 215 BULK TELEPHONY METADATA PROGRAM

28. The Declaration of Teresa H. Shea, dated October 1, 2013, provides a detailed description of the Program's value to the protection of national security, which would be lost (or substantially degraded) during any period of time that compliance with an injunction issued in this case required the cessation of collection or analytic queries of bulk metadata under the Program.

29. Passage of the USA FREEDOM Act does not mitigate the resulting harm to national security for any period prior to November 29, 2015, the date when additional authorities that enable the query-at-the-provider model become effective.

30. Furthermore, an injunction requiring or resulting in the cessation of all access to bulk metadata collected under the Program, even technical access, would have adverse consequences for the NSA's implementation of the new targeted query-at-the-provider program authorized under the USA FREEDOM Act. The Government has requested that the FISC approve continued access by technical personnel to the historical bulk metadata collected under the Program until February 29, 2016. The purpose of this access is solely to verify the completeness and accuracy of records produced under the new query-at-the-provider program. The ability to query the historical bulk metadata acquired under the Program is an important step to bringing on-line the new production mechanism authorized by Congress, assuring the proper function of that system, and verifying its ability to serve an important national security function.

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

DATE: 1 Oct 2015

Gregg C. Potter
Major General, U.S. Army
Signals Intelligence Deputy 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

15 - 99

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: ~~28 August 2040~~

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, which meet the definition of minimization procedures in 50 U.S.C. § 1861(g). *See* 50 U.S.C. § 1861(c)(1), as amended by the USA FREEDOM Act of 2015. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number BR 15-75 and its predecessors. [50 U.S.C. § 1861(c)(1)]

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 IN PART, 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]

(1) B. The Custodian of Records of [redacted] shall produce to NSA upon service of the

[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).

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" created by [redacted] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [redacted]

[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 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 or has received as a result of this Order or predecessor Orders of this Court requiring the production to NSA of telephony metadata pursuant to 50 U.S.C. § 1861 ("BR metadata"), NSA shall strictly adhere to the limitations and procedures set out at subparagraphs A. through G. below. Furthermore, after November 28, 2015, the Government shall not access BR metadata for intelligence analysis purposes.

A. The Government is hereby prohibited from accessing 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 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-

[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 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]

approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes, 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. The Government may request, by motion and on a case-by-case basis, permission from the Court for NSA[5] to use specific selection terms that satisfy the

[redacted]

[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.

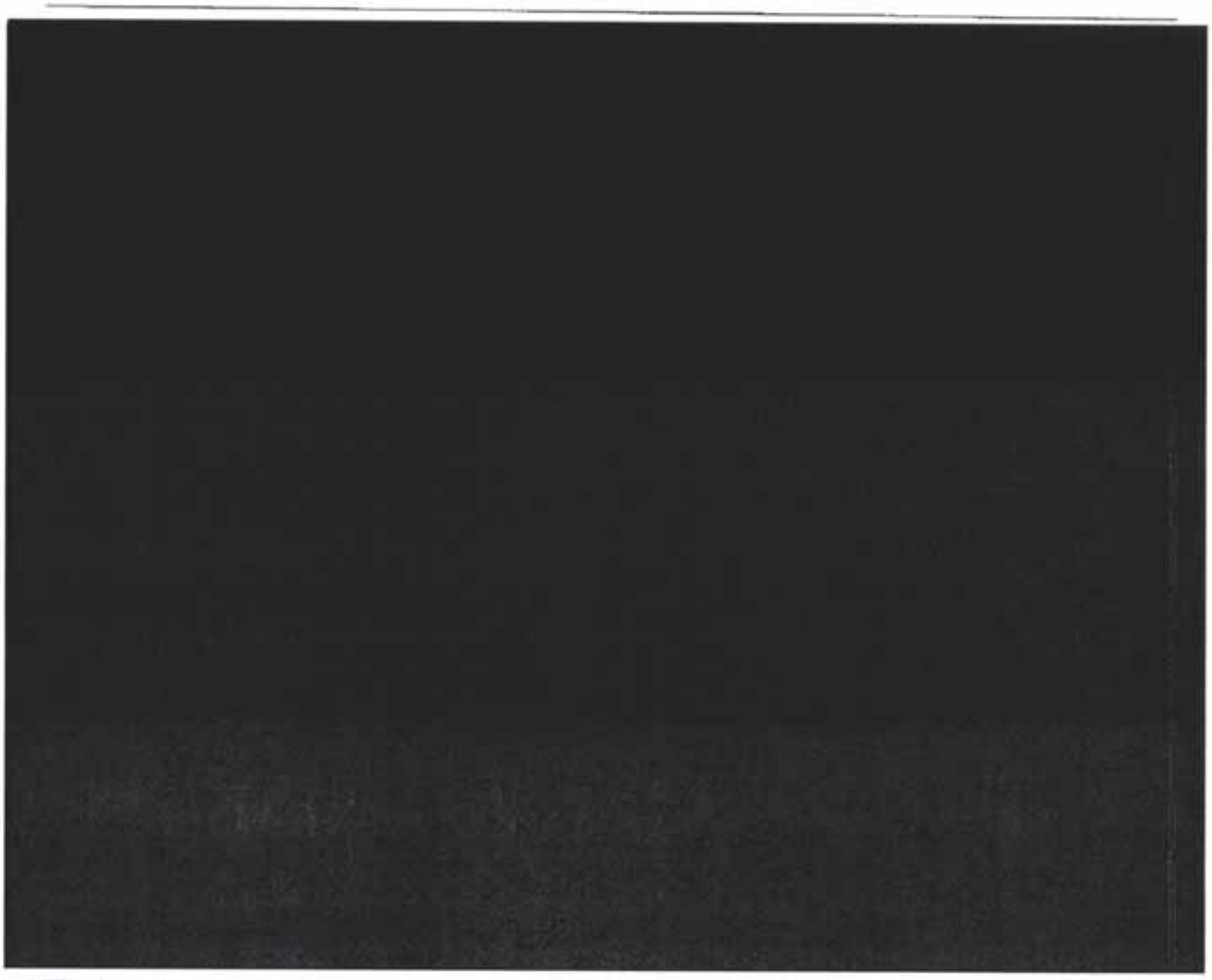
reasonable articulable suspicion (RAS) standard[6] as "seeds" to query the BR metadata for purposes of obtaining foreign intelligence information. The Government may query

---

[6] The reasonable articulable suspicion (RAS) standard is met when, 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 that the selection term to be queried is associated with [redacted] provided, however, that any selection term reasonably believed to be used by a United States (U.S.) person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution. For purposes of this Order, the term [redacted]

[redacted]

the BR metadata to obtain contact chaining information within two hops of an approved "seed."[7] In addition, the Director or Acting Director of NSA may authorize the emergency querying of the BR metadata with a selection term for purposes of obtaining foreign intelligence information, within two hops of a "seed," if: (1) the Director or Acting Director of NSA reasonably determines that an emergency situation



[7] The first "hop" from a seed returns results including all identifiers (and their associated metadata) with a contact and/or connection with the seed. The second "hop" returns results that include all identifiers (and their associated metadata) with a contact and/or connection with an identifier revealed by the first "hop."

exists with respect to the conduct of such querying before an order authorizing such use of a selection term can with due diligence be obtained; and (2) the Director or Acting Director of NSA reasonably determines that the RAS standard has been met with respect to the selection term.[8] In any case in which this emergency authority is exercised, the Government shall make a motion in accordance with the Primary Order to the Court as soon as practicable, but not later than 7 days after the Director or Acting Director of NSA authorizes such query.[9]

(i) Any submission to the Court under this emergency provision shall, at a minimum, specify the selection term for which query authorization is sought or was granted, provide the factual basis for the NSA's belief that the reasonable articulable suspicion standard has been met with regard to that selection term and, if such query has already taken place, a statement of the emergency necessitating such query.[10]

---

[8] Before an emergency query is performed under this authority, NSA's Office of General Counsel (OGC), in consultation with the Director or Acting Director, shall confirm 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.

[9] In the event the Court denies such motion, the Government shall take appropriate remedial steps, including any steps the Court may direct.

[10] For any selection term that is subject to ongoing Court-authorized electronic surveillance, pursuant to 50 U.S.C. § 1805, based on this Court's finding of probable cause to believe that the selection term is being used or is about to be used by agents of [redacted] including those used by U.S. persons, the Government may use such selection terms as "seeds" during any period of ongoing Court-authorized electronic surveillance without first seeking authorization

(ii) NSA shall ensure, 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.[11] 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.[12]

(iii) The Court's finding that a selection term is associated with [redacted] shall be effective until November 28, 2015, at 11:59 p.m. Eastern Time.[13]

---

from this Court as described herein. Except in the case of an emergency, NSA shall first notify the Department of Justice, National Security Division of its proposed use as a seed any selection term subject to ongoing Court-authorized electronic surveillance.

[11] The Court understands that NSA has implemented technical controls that preclude any query for intelligence analysis purposes with a non-RAS-approved seed. In cases of imminent threat to human life NSA may bypass these technical controls, subject to management controls, to conduct queries using RAS-approved seeds that have been blocked by technical restraints.

[12] This auditable record requirement shall not apply to further accessing of the results of RAS-approved queries.

[13] The Court understands that from time to time the information available to NSA 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, the Government's submission shall specify the time frame for which the selection term is or was associated with [redacted] In the event that the RAS standard is met, analysts conducting manual queries using that selection term shall properly minimize information that may be returned within query results that fall outside of that timeframe.

The Court understands that NSA received 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 Order, [redacted]

(iv) Queries of the BR metadata using RAS-approved selection terms for purposes of obtaining foreign intelligence information may occur by manual analyst query only. Queries of the BR metadata to obtain foreign intelligence information shall return only that metadata within two "hops" of an approved seed.

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 receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.[14] 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,

[redacted]

[14] 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.

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.[15] 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 personnel (1) in order to enable them to determine whether the information may be exculpatory or otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions. Notwithstanding the above requirements, NSA may share the results from intelligence analysis queries of the BR metadata, including United States person information, with Legislative Branch personnel to facilitate lawful oversight functions.

E. The Application requests authority for the Government to retain BR metadata after November 28, 2015, in accordance with the Opinion and Order of this Court issued on March 12, 2014 in docket number BR 14-01, and subject to the conditions stated therein, including the requirement to notify this Court of any material developments in

[15] 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.

civil litigation pertaining to such BR metadata. The Application also requests authority, for a period ending on February 29, 2016, for appropriately trained and authorized technical personnel (described in subparagraph B. above) to access BR metadata to verify the completeness and accuracy of call detail records produced under the targeted production orders authorized by the USA FREEDOM Act. The Court is taking these requests under advisement and will address them in a subsequent order or orders. Accordingly, this Primary Order does not authorize the retention and use of BR metadata beyond November 28, 2015.

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.[16] OGC shall provide NSD/DoJ with copies 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 prior to the expiration of the authority requested herein.

---

[16] 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.

(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.

(vi) Prior to implementation of any automated query processes, such 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 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, other than Executive Branch or Legislative Branch personnel receiving such results for their purposes that are exempted from the dissemination requirements of paragraph (3)D above. 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 counterterrorism information or to assess its importance.

(4) The Court recognizes that there are two cases involving challenges to the legality of this collection pending before federal appellate courts, *Klayman v. Obama*, No.

14-5004 (D.C. Cir. argued Nov. 4, 2014), and *Smith v. Obama*, No. 14-35555 (9th Cir. argued Dec. 8, 2014), and one case in which a federal appeals court panel has issued an opinion regarding the legality of this collection, *A.C.L.U. v. Clapper*, No. 14-42 (2d Cir. May 7, 2015).[17] If an opinion is issued in any of the two pending cases prior to the expiration of this Order, the government is directed to inform the Court promptly if the government's implementation of this Order has changed as a result of such opinion(s). The government also is directed to inform the Court promptly if the government's implementation of this Order has changed as a result of the opinion in *A.C.L.U. v. Clapper*.

-- *Remainder of page intentionally left blank.* --

[17] By letter dated June 10, 2015 in docket number Misc. No. 15-01, the government notified the Court that on June 9, 2015 the federal appeals court panel entered an order which directed the parties in that litigation to submit supplemental briefs regarding the effect of the USA FREEDOM Act on the case and "in particular whether any or all of the claims asserted by the plaintiffs-appellants have been rendered moot as a result of that legislation." The order also stayed issuance of the court's mandate pending the parties' supplemental briefing and extended the deadline for the submission of any petitions for rehearing. The Court understands that on July 14, 2015, the ACLU filed a Motion for Preliminary Injunction in which it also presented arguments regarding the effect of the USA FREEDOM Act on the case; and that on July 27, 2015, the government filed a Combined Supplemental Brief for Appellees and Opposition to Motion for Preliminary Injunction. The Court further understands that as of the date of this Order, the Second Circuit panel has not issued any additional relevant opinions or orders. If an additional opinion or order is issued prior to the expiration of this Order, the government is directed to inform the Court promptly if the government's implementation of this Order has changed as a result of any such opinion or order.

This authorization regarding [redacted] expires on the 28th day of November, 2015, at 11:59 p.m., Eastern Time.

Signed 27 Aug. '15 3:19pm Eastern Time
Date Time

MICHAEL W. MOSMAN
Judge, United States Foreign
Intelligence Surveillance Court

I, [redacted] Chief Deputy Clerk, FISC, certify that this document is a true and correct copy of the original
[redacted]

EXHIBIT B

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

MAY 20 2015

The Honorable Mitch McConnell
Majority Leader
United States Senate
Washington, DC 20510

The Honorable Harry Reid
Minority Leader
United States Senate
Washington, DC 20510

Dear Senators McConnell and Reid:

The USA Freedom Act would establish a 180-day period for transitioning from the current bulk-collection program for telephone metadata to a model where queries would be carried out against business records held by telephone service providers. Several questions have been raised about the feasibility of the 180-day deadline.

Should the USA Freedom Act of 2015 become law, NSA assesses that the transition of the program to a query at the provider model is achievable within 180 days, with provider cooperation. We base this judgment on the analysis that we have undertaken on how to make this model work. Upon passage of the law, we will work with the companies that are expected to be subject to Orders under the law by providing them the technical details, guidance, and compensation to create a fully operational query at the provider model. We are aware of no technical or security reasons why this cannot be tested and brought on line within the 180-day period.

We very much appreciate the time and attention the Senate continues to devote to this important issue.

MICHAEL S. ROGERS
Admiral, U.S. Navy
Director, National Security Agency