

Approved for public release May 5, 2014

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

1 STUART F. DELERY
 Assistant Attorney General
 2 JOSEPH H. HUNT
 Director, Federal Programs Branch
 ANTHONY J. COPPOLINO
 3 Deputy Branch Director
 JAMES J. GILLIGAN
 4 Special Litigation Counsel
 MARCIA BERMAN
 5 Senior Trial Counsel
 BRYAN DEARINGER
 6 RODNEY PATTON
 Trial Attorneys
 7 U.S. Department of Justice
 Civil Division, Federal Programs Branch
 8 20 Massachusetts Avenue, N.W.
 Washington, D.C. 20001
 9 Phone: (202) 514-4782
 Fax: (202) 616-8460

*Attorneys for the United States and
Government Defendants Sued in their
Official Capacities*

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

CAROLYN JEWEL, *et al.*

No. 08-cv-4373-JSW

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*

Defendants.

FIRST UNITARIAN CHURCH OF LOS
ANGELES, *et al.*,

No. 13-cv-3287-JSW

Plaintiffs,

**CLASSIFIED DECLARATION
OF TERESA H. SHEA**

v.

**EX PARTE, IN CAMERA
SUBMISSION**

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Date: March 19, 2014
Time: 2:00 P.M.
Courtroom: 11 – 19th Floor
Judge Jeffrey S. White

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

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

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

(U) INTRODUCTION

1
2 1. (U) I am the Director of the Signals Intelligence Directorate (SID) at the National
3 Security Agency (NSA), an intelligence agency within the Department of Defense (DoD). I am
4 responsible for, among other things, protecting NSA Signals Intelligence activities, sources, and
5 methods against unauthorized disclosures. Under Executive Order No. 12333, 46 Fed. Reg.
6 59941 (1981), as amended on January 23, 2003, 68 Fed. Reg. 4075 (2003), and August 27, 2004,
7 69 Fed. Reg. 53593 (2004), and August 4, 2008, 73 Fed. Reg. 45325, the NSA is responsible for
8 the collection, processing, and dissemination of Signals Intelligence information for foreign
9 intelligence purposes of the United States. I have been designated an original TOP SECRET
10 classification authority under Executive Order 13526, 75 Fed. Reg. 707 (Jan. 5, 2010), and
11 Department of Defense Directive No. 5200.1-R, Information Security Program (Feb. 24, 2012).

12 2. (U) My statements herein are based upon my personal knowledge of Signals
13 Intelligence collection and NSA operations, information available to me in my capacity as
14 Signals Intelligence Director, and the advice of counsel.

15 3. (U) This declaration is classified TOP SECRET//SI//NOFORN pursuant to the
16 standards in Executive Order 13526, 3 C.F.R. 298 (2009). Under Executive Order 13526,
17 information is classified "TOP SECRET" if disclosure of the information reasonably could be
18 expected to cause exceptionally grave damage to national security, "SECRET" if disclosure of
19 the information reasonably could be expected to cause serious damage to national security, and
20 "CONFIDENTIAL" if disclosure of the information reasonably could be expected to cause
21 identifiable damage. In addition to classified information, this declaration also references
22 Special Intelligence (SI), which is a subcategory of Sensitive Compartmented Information (SCI),
23 for which the Director of National Intelligence (DNI) imposes additional safeguards and access
24 requirements. At the beginning of each paragraph of this declaration, the letter or letters in
25 parentheses designate(s) the degree of sensitivity of the information contained in the paragraph.

26 4. (U) When used for this purpose, letters "U," "C," "S," and "TS" indicate, that the
27 information is UNCLASSIFIED, or is classified CONFIDENTIAL, SECRET, or TOP SECRET,
28

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

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

1 respectively. Where "SI" information is at issue in the paragraph, these letters will follow after
2 the classification letters.

3 5. (U) Finally, and in addition to the separate levels of classification markings defined
4 by Exec. Order 13526, there are also dissemination controls appropriately associated with
5 classified information. Dissemination control markings identify the expansion or limitation on
6 the distribution of the information. Not Releasable to Foreign Nationals, indicated by the
7 abbreviation NOFORN or NF, is an explicit foreign release marking used to indicate that the
8 information may not be released in any form to foreign governments, foreign nationals, foreign
9 organizations, or non-US citizens without permission of the originator of the information.

10 6. (U) Accordingly, none of the information in this declaration can be removed from
11 classified channels without prior review by NSA and cannot appear in the public record,
12 including the docket reflecting these proceedings.

13 **(U) DESTRUCTION OF COLLECTED TELEPHONY METADATA IN COMPLIANCE**
14 **WITH FISC MINIMIZATION REQUIREMENTS**

15 7. (U) Under the "business records" provision of the Foreign Intelligence Surveillance
16 Act ("FISA"), 50 U.S.C. § 1861, as enacted by section 215 of the USA Patriot Act, Pub. L. No.
17 107-56, 115 Stat. 272 (2001) ("Section 215"), the Foreign Intelligence Surveillance Court
18 ("FISC"), upon application by the Federal Bureau of Investigation (FBI), may issue an order "for
19 the production of any tangible things (including books, records, papers, documents, and other
20 items) for an investigation [1] to obtain foreign intelligence information not concerning a United
21 States person or [2] to protect against international terrorism." 50 U.S.C. § 1861(a)(1). Since
22 May 2006, the NSA has collected bulk telephony metadata ("data") pursuant to FISC orders
23 directing certain telecommunications service providers to produce to the NSA on a daily basis
24 electronic copies of "call detail" records¹ created by the recipient providers for calls to, from, or
25 wholly within the United States. Under the FISC's orders, the NSA's authority to continue
26 collecting the data expires after approximately 90 days and must be renewed. The FISC has

27 ¹~~(TS//SI//NF)~~ Under the terms of the FISC's orders, this data includes, as to each call, the telephone
28 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.

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

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

1 renewed the daily collection of these data approximately every 90 days since May 2006 based on
2 applications from the FBI, supported by the NSA, showing that the production of these call detail
3 records satisfies the requirements of Section 215. To protect U.S. person information the FISC's
4 orders impose procedures to minimize access to, use, dissemination, and retention of the data
5 consistent with the need to acquire, produce, and disseminate foreign intelligence information.
6 Among these is the requirement to destroy all bulk telephony metadata obtained under the
7 FISC's Section 215 orders within five years (60 months) of the data's collection. This five-year
8 limit reflects the judgment arrived at by the Executive Branch that after five years the data no
9 longer holds significant foreign intelligence value meriting their retention.


10 8. ~~(TS//SI//NF)~~ The NSA effectuates this retention limit using existing computer systems
11 architecture (referred to herein as the "existing architecture") by implementing [REDACTED]
12 compliance process during which the NSA destroys the data to be aged off [REDACTED]
13 [REDACTED] beforehand. Thus,
14 at any given time the NSA has [REDACTED] worth of data, but not more than five
15 years. [REDACTED]

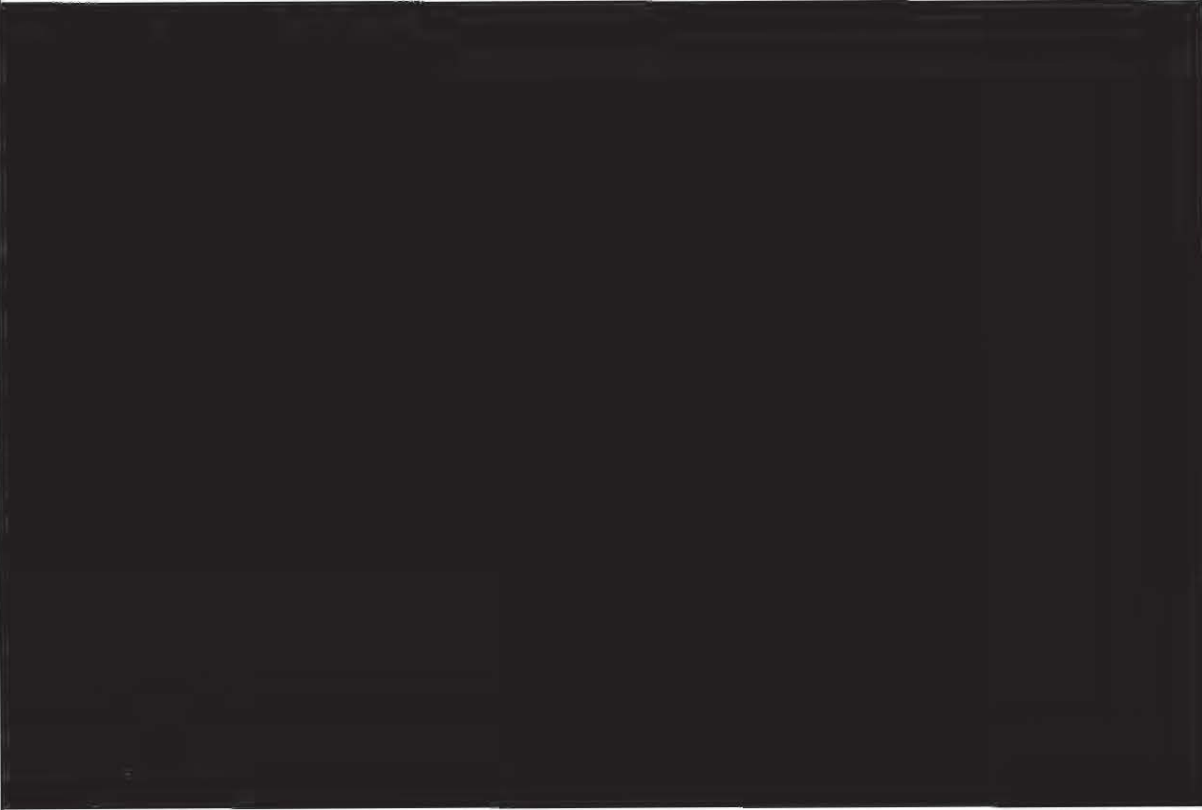
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED] NSA intelligence analysts do not and will not have access to any data that

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

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

1 are otherwise subject to the FISC-imposed destruction requirement while the question of whether
 2 the data must be preserved for litigation purposes is being resolved. Nor would they have access
 3 to the data afterward if they are preserved.²

4 9. ~~(TS//SI//NF)~~ The NSA has for several years been in the process of developing a new
 5 computer systems architecture (referred to herein as the “new architecture”) for storing and
 6 processing the telephony metadata collected pursuant to the FISC’s orders under Section 215.
 7 The purpose of this new architecture is to better ensure compatibility with NSA-wide
 8 information technology upgrades. 

9 

10

11

12

13

14

15

16

17

18

19

20

21

22

23 10. (U) I have been informed that Plaintiffs in these actions have requested that the
 24 Government be required to preserve the “telephone records” that the NSA has collected under
 25 the FISC-authorized telephony metadata program. This request could be taken to mean either
 26 (i) targeted preservation of metadata collected under Section 215 that pertain only to the

27 ² (U) By order of the FISC on March 12, 2014, NSA technical personnel may access the metadata only for
 28 the purpose of ensuring continued compliance with the Government’s preservation obligations to include taking
 reasonable steps designed to ensure appropriate continued preservation and/or storage, as well as the continued
 integrity of the BR metadata.

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

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

1 Plaintiffs' telephone calls, if any, or (ii) mass retention of all the data that are more than five
 2 years old. Both tasks would impose significant financial burdens on the NSA, divert personnel
 3 and technological resources from performance of the NSA's national security mission, and
 4 present other issues as well. I discuss each task in turn.

5 **(U) CONTINUED RETENTION OF COLLECTED TELEPHONY METADATA, IF**
 6 **ANY, RELATED TO PLAINTIFFS' TELEPHONE CALLS**

7 11. ~~(TS//SI//NF)~~ To the extent Plaintiffs seek targeted preservation of data associated
 8 only with their own telephone calls, the NSA first would have to determine whether it has ever
 9 collected data pursuant to Section 215 associated with Plaintiffs' calls. For the NSA to make this
 10 determination, each Plaintiff organization and each individual Plaintiff would have to provide the
 11 NSA with, for example, all telephone numbers they were assigned or used at any time during the
 12 period for which data that otherwise would be destroyed must be preserved [REDACTED]
 13 [REDACTED]

14 The Plaintiffs would also have to inform the NSA of the specific time period during which they
 15 were assigned or used each telephone number, so that data pertaining to the calls of other persons
 16 who may have used or been assigned a particular number are not inadvertently retained. For the
 17 same reason, if this litigation continues long enough, each Plaintiff would have to inform the
 18 Government of any changes in the numbers they use or are assigned.

19 12. (U) It is also important to note that the NSA would not simply be preserving data
 20 consisting of the Plaintiffs' phone numbers; the preserved data would include, among other
 21 information, the initiating and receiving number, and the date, time, and duration of each call in
 22 each record that was collected. For example, if a call detail record concerning a phone call made
 23 by a Plaintiff was collected, that Plaintiff's telephone number as well as the receiving number—
 24 which may be that of an individual not in any way associated with these lawsuits—would be
 25 preserved together, along with the date, time, and duration of that individual's call with the
 26 Plaintiff.

27 13. (U) Moreover, pursuant to the FISC's orders, NSA intelligence analysts may not
 28 access the data except through queries conducted for foreign intelligence purposes using

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

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

1 identifiers (e.g., telephone numbers) that are reasonably suspected of being associated with
2 foreign terrorist organizations that have been approved for targeting by the FISC. Therefore,
3 even if Plaintiffs were to provide the NSA with the telephone numbers they used or were
4 assigned during the relevant time period, to identify records of Plaintiffs' calls would possibly
5 require prohibited queries of the database for purposes other than obtaining foreign intelligence
6 information by using identifiers (Plaintiffs' telephone numbers) that have not been approved
7 under the "reasonable, articulable suspicion" standard. This means that, before determining
8 whether the NSA has collected metadata associated with Plaintiffs' calls, the Government may
9 first have to seek and obtain approval from the FISC to run queries in the NSA's database for
10 records associated with each telephone number provided by each Plaintiff. In the event that data
11 associated with any calls made by Plaintiffs have been collected by the NSA, the queries, among
12 other things, will return—and, in accordance with any preservation obligation imposed by the
13 Court, the NSA would separately maintain—a collection of records indicating the telephone
14 numbers with which each Plaintiff was in contact over a period of one or more years, depending
15 on how long the NSA must continue to preserve data it would otherwise destroy.

16 14. (U) In addition to the foregoing considerations are the time, effort, and resources
17 that would be required for the NSA to preserve until the conclusion of the litigation any data
18 (whether pertaining to Plaintiffs' calls only or not) that would otherwise have been destroyed in
19 compliance with the FISC's five-year retention limit. The fact that there is no way to predict
20 how long the lawsuits before this Court will last, coupled with ever-changing mission
21 requirements and systems, makes it extremely difficult to estimate costs and to devise the most
22 cost-effective data storage solution should this Court issue an order requiring preservation of
23 data that would otherwise be subject to age-off. All of the feasible solutions present the
24 possibility of imposing substantial cost burdens on the NSA that would divert limited resources
25 away from foreign intelligence mission requirements. While it is impossible to quantify the
26 additional risks such a diversion of resources may pose to the national security, I deem such risks
27 to be significant.

28 15. (U) An order to preserve only metadata pertaining to Plaintiffs' calls (assuming such

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

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

1 data have been collected) would require the NSA to devote significant financial and personnel
2 resources over several months—assets that would otherwise be devoted to the NSA’s national
3 security mission—to create, test, and implement a solution that would preserve only these
4 targeted data on an ongoing basis.

5 16. ~~(TS//SI//NF)~~ Specifically, with regard to the new architecture, which is currently
6 scheduled to replace the existing architecture later this year, the NSA would need to assign a
7 team of NSA software developers, already familiar with the Section 215 telephony metadata
8 program and the relevant platform, to create and design appropriate software and write the
9 source code that would allow the NSA to identify and separately retain the telephony metadata
10 associated only with Plaintiffs’ telephone numbers, if any, that would otherwise be aged off and
11 destroyed on a daily basis. Once the software had been created, this NSA team would need to
12 test and verify that the program works as intended, resolve any flaws or bugs, and then (as with
13 any significant modification to an existing architecture) seek and obtain approvals within the
14 NSA for implementation of the new software program. I estimate, based on the information
15 available to me now, that this process would take the team of NSA software developers [REDACTED]
16 [REDACTED] of full-time work on the project from deployment to operational capability. The
17 cost of this process is difficult to quantify in the abstract, but I would estimate that the initial cost
18 would be at least [REDACTED]. Additional costs would accrue over time. Over the course of three
19 years, I estimate the total cost, including for the aforementioned labor, hardware maintenance,
20 back up media, and additional software maintenance, would be at least [REDACTED]. Over five
21 years, I estimate the total cost would be at least [REDACTED]. I emphasize that these are
22 preliminary estimates. Additional time would be needed in order to develop more complete and
23 accurate estimates. Based on past experience, I believe that costs could well exceed these
24 estimates and the estimates that follow in subsequent paragraphs of my declaration. In addition
25 to the inherent difficulty of finding sufficient funds in the NSA’s budget to cover such
26 unanticipated costs, mission-enhancing functions would be delayed or impaired while resources
27 are diverted to the preservation effort. For example, the software developers needed for this
28 effort would be unable to work on NSA mission requirements during this [REDACTED]

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

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

1 period, causing delay in making the new architecture operational.

2 17. ~~(TS//SI//NF)~~ Hiring contractors or assigning other software developers who are not
3 familiar with the Section 215 program or the new architecture to resolve this issue is not a viable
4 option. The platform for the new architecture is proprietary and was developed by the NSA for
5 purposes of the Section 215 program. Without devoted personnel who are experienced with the
6 platform and its software, this process would take [REDACTED] (instead of [REDACTED]
7 [REDACTED] to allow for the additional training to assure successful completion of the work.

8 18. ~~(TS//SI//NF)~~ With regard to the existing architecture, NSA would be required, in
9 order to preserve any metadata associated with Plaintiffs' calls that may have been collected and
10 stored in that platform, to create, design, and write a software program that would allow the NSA
11 to query the data for records associated with Plaintiffs' telephone numbers. Once responsive
12 data, if any, were identified, NSA would then need to extract that data from the analytic
13 databases and store it separately in an appropriate format. I estimate that the initial costs for
14 personnel time and hardware alone would be at least [REDACTED] Over three years, I estimate the
15 total cost, including for personnel time and hardware, would be well in excess of [REDACTED]
16 Over five years, I estimate the total cost would be at least [REDACTED] Again, I emphasize that
17 these are preliminary estimates. Depending on when the transition to the new architecture
18 occurs, additional costs to preserve data in the existing architecture and maintain some or all of
19 the additional architecture may also accrue.

20 19. ~~(TS//SI//NF)~~ In sum, based on the foregoing, I estimate that, if the Court orders the
21 Government to preserve metadata associated with Plaintiffs' calls, the initial cost would be [REDACTED]
22 [REDACTED] and at least approximately [REDACTED] Over three years, I estimate the total cost would
23 be approximately [REDACTED] and possibly more. Over five years, I estimate the total cost would
24 be well in excess of [REDACTED] These preliminary cost estimates are in monetary terms only
25 and do not factor in the diversion of personnel and technological resources from the NSA's
26 foreign intelligence mission.


27
28

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

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

1 **(U) RETENTION OF ALL "AGED OFF" TELEPHONY METADATA FOR THE**
2 **DURATION OF THE LITIGATION**

3 20. ~~(TS//SI//NF)~~ The alternative to identifying, extracting, and preserving metadata
4 pertaining just to Plaintiffs' telephone calls would be to preserve all telephony metadata
5 collected more than five years ago in a format that precludes any access or use by NSA
6 personnel for any purpose other than ensuring continued compliance with the Government's
7 preservation obligations (to include taking reasonable steps designed to ensure appropriate
8 continued preservation and/or storage, as well as the continued integrity of the data.)

9
10
11
12
13
14
15 21. ~~(TS//SI//NF)~~ As described below, all data retained beyond the five-year retention
16 limit specified in the FISC's orders could be preserved either by (i) maintaining all the data,
17  on a non-analytic portion of the existing architecture's
18 software and hardware, or (ii) by migrating the all the data to backup tapes. Under either option,
19 preservation of all telephony metadata retained beyond the five-year limit imposed by the FISC
20 would involve substantial costs to the agency, financial and otherwise, either to preserve or to
21 access the data (for litigation purposes). The first method of preservation would involve more
22 costs initially but fewer costs to make the data retrievable. The second method would involve
23 fewer upfront costs, but it would be significantly more expensive to retrieve the data and make
24 them searchable for litigation purposes should that become necessary.

25 22. ~~(TS//SI//NF)~~ Regardless of whether NSA preserves the data using the existing
26 architecture or by migrating the data to backup tapes, there is no way to guarantee with absolute
27 certainty that over the course of time, the integrity of the data will be preserved. As a general
28 matter, the longer the time that electronic data must be preserved, the greater the risk that such

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

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

1 data—in spite of best efforts by NSA personnel—will become unusable for litigation or for any
2 other purpose.

3 **(U) Option One**

4 23. ~~(TS//SI//NF)~~ The first of the two options for preserving all of the data would involve
5 migrating the data into a preservation system to which NSA intelligence analysts would have no
6 access for any purpose. Further, some portion of the existing architecture, instead of being
7 decommissioned, as is now planned for [REDACTED] would remain in operation for the sole
8 purpose of preserving the data for civil litigation purposes.

9 24. ~~(TS//SI//NF)~~ [REDACTED]

10 [REDACTED]

11 [REDACTED]

12 [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 25. ~~(TS//SI//NF)~~ An important goal of the evolution from the existing architecture to the
16 new architecture is to realize cost savings through [REDACTED]

17 [REDACTED] A significant portion of those savings will be lost if the
18 existing architecture cannot be decommissioned, as planned, once the new architecture becomes
19 operational.

20 26. ~~(TS//SI//NF)~~ For example, continued operation of the hardware on which the
21 existing architecture is located will require the NSA to continue to devote space in which to
22 house the hardware, as well as electrical power needed to operate and cool it. These are critical
23 resources, all in great demand at NSA given the breadth of the agency's responsibilities for the
24 acquisition, analysis, and dissemination of foreign intelligence information. Continuing to
25 devote these resources to the operation of the existing architecture for litigation purposes will
26 mean diverting them, in effect, from ongoing (or intended) signals intelligence operations with a
27 corresponding impact on the NSA's ability to collect, process, analyze, and disseminate foreign
28 intelligence information for purposes of national security. In addition, preservation of data in the

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

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

1 existing architecture would require a diversion of qualified personnel resources from other NSA
2 operational missions to maintain and repair the hardware and ensure the continued integrity of
3 the stored data. Over the next year, I estimate the cost of this undertaking in monetary terms
4 alone to be [REDACTED] and in the range of up to or exceeding [REDACTED]. I
5 emphasize that this is a preliminary estimate and the actual expenses may vary substantially from
6 this figure if the Court ordered this option.

7 **(U) Option Two**

8 27. ~~(TS//SI//NF)~~ An alternative to the preservation of telephony metadata within the
9 existing architecture would be to migrate data acquired more than five years ago from online
10 databases to offline storage on tape. Under this option, all data would be copied onto sets of
11 tapes for offline storage. [REDACTED]

12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 28. ~~(TS//SI//NF)~~ Preservation of the data once they have been transferred onto tapes
21 would not involve a diversion of financial, technological, and personnel resources on the same
22 scale as preserving the data on an active, repurposed system within the existing architecture.
23 Nevertheless, the cost remains substantial. Once metadata have been transferred to offline
24 storage, the tapes containing the data would have to be maintained under appropriate
25 environmental conditions (temperature and humidity) to maintain the integrity of the media and
26 the preserved data. The estimated cost of this method would be approximately [REDACTED] per
27 year simply to store the data without ever retrieving it. I emphasize that this is a preliminary
28 estimate and the actual expenses may vary substantially from this figure.

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

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

1 29. ~~(TS//SI//NF)~~ These costs would greatly increase if the NSA were required to retrieve
 2 these data for litigation purposes. To make the data preserved on tapes accessible for possible
 3 purpose of discovery in litigation (e.g., to search for records of calls to or from the Plaintiffs) at a
 4 later date, would require substantial time and effort and impose additional significant costs on
 5 the NSA.

6
 7
 8
 9
 10
 11 I emphasize that this is a preliminary
 12 estimate and actual expenses may vary substantially from this figure. The larger the amount of
 13 data that is preserved over time, the greater will be the time for needed and cost to the agency of
 14 making the data accessible in this fashion. As with any type of tape storage, there is also a risk
 15 that the integrity of the data could be compromised through the passage of time, and that the data
 16 may not be retrievable or searchable if the existing architecture cannot be made functional again.

17 **(U) PRESERVATION OF OTHER POTENTIAL EVIDENCE**

18 30. (U) I understand that the Plaintiffs have inquired what steps the Government has
 19 taken to preserve telephony metadata, Internet metadata, and communications content collected
 20 by the NSA under authority of the President following the September 11, 2001, terrorist attacks,
 21 and thereafter under FISC authority pursuant to sections 402, 501, and 702 of FISA, as well as
 22 other documents and information pertaining to those activities. I address those matters below.
 23 Nothing stated herein, however, is intended to be, or should be construed as, an admission either
 24 (i) that documents and information pertaining to activities carried out under FISC authority,
 25 including the data collected, are relevant to the *Jewel* litigation (or its companion case, *Shubert v.*
 26 *Obama*), or (ii) that documents and information pertaining to the collection of Internet metadata
 27 and communications content under FISC authority pursuant to sections 402 and 702 of FISA,
 28 including the data collected, are relevant to the *First Unitarian* litigation.

31. (U) The steps taken by the Government to identify and to preserve documents and

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

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

1 information related to the particular intelligence activities authorized by the President in the
2 wake of the September 11 attacks are described in the Government's Classified Supplemental
3 Memorandum in Opposition to the Plaintiff's Motion for Order to Preserve Evidence, dated
4 October 25, 2007, filed in the case styled *In re NSA Telecommunications Records Litigation*,
5 MDL Dkt. No. 06-1791-VRW. The Government supported its Memorandum with the Classified
6 *in Camera, Ex Parte* Declaration of ██████████ Deputy Chief of Staff for Operations and
7 Support, Signals Intelligence Division, National Security Agency to apprise the Court of the
8 preservation efforts that the Government had undertaken. A declassified version of the
9 Government's memorandum and ██████████ declaration have been prepared for public filing in
10 this litigation. As explained in ██████████ declaration the NSA had at that time preserved, and
11 the NSA continues to preserve, among other things, certain Internet and telephony metadata
12 collected and the content of certain communications intercepted, under Presidential authority, in
13 connection with the NSA intelligence programs known collectively as the President's
14 Surveillance Program.

15 32. (U) It is not feasible in the time available to respond to Plaintiffs' Opening Brief re:
16 Evidence Preservation to describe in detail the various steps that the NSA has taken to preserve
17 documents and information related to the bulk collection of Internet and telephony metadata, and
18 the collection of communications content, under FISC authority pursuant to sections 402 and 702
19 of FISA. With respect, however, to the retention of the collected data themselves, I can advise
20 the Court as follows.

21 33. ~~(TS//SI//NF)~~ As discussed above, the FISC's orders authorizing the NSA's bulk
22 collection of telephony metadata under FISA section 501 (Section 215) require that metadata
23 obtained by the NSA under this authority be destroyed no later than five years after their
24 collection. To comply with this legal requirement, the NSA between ██████████ of 2011,
25 destroyed all the metadata collected between May 2006 (the inception of the program under
26 FISC authorization) ██████████ Between ██████████ of 2012, the NSA destroyed all
27 the metadata collected between ██████████ 2007, ██████████ Between ██████████ of
28 2013, the NSA destroyed all the metadata collected between ██████████ 2008 ██████████
with the exception of the test data, collected between ██████████ 2009. In accordance

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

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

1 with the Court's March 10, 2014, order, and the subsequent March 12, 2014, order of the FISC,
2 the scheduled destruction of the data collected between [REDACTED] 2009 [REDACTED] has
3 been put on hold pending further order of this Court. Therefore, the NSA currently retains bulk
4 telephony metadata collected under FISC authority between [REDACTED] 2009 [REDACTED]
5 and such data between [REDACTED] 2009 and the present.

6 34. ~~(TS//SI//NF)~~ The NSA's collection of bulk Internet metadata transitioned to FISC
7 authority under section 402 of FISA in July 2004. Until December 2009, these data were subject
8 under the FISC's orders to a 4.5-year retention limit, after which, pursuant to a change in the
9 FISC orders, these data could be retained for up to five years. In December 2011, the
10 Government decided not to seek FISC reauthorization of the NSA's bulk collection of Internet
11 metadata because the program had not met operational expectations. Because the NSA did not
12 intend thereafter to use the Internet metadata it had retained for purposes of producing or
13 disseminating foreign intelligence information, in keeping with the principle underlying the
14 destruction requirements imposed by the FISC, the NSA destroyed the remaining bulk Internet
15 metadata in December 2011.

16 35. ~~(TS//SI//NF)~~ Certain of the NSA's acquisition of telephone and Internet content
17 under Presidential authorization similarly transitioned to FISC authority. Beginning on
18 January 10, 2007, the FISC issued orders (known as the "Foreign Telephone and Email Order"
19 and [REDACTED] authorizing the Government to conduct certain electronic
20 surveillance activities that had been occurring under the authority of the President. Presidentially
21 authorized surveillance activities expired shortly thereafter. The FISC orders authorizing the
22 electronic surveillance required that communications acquired under those authorities be
23 destroyed no later than five years after their collection. All NSA intelligence reports utilizing the
24 content of communications intercepted under authority of these orders are preserved
25 permanently.

26 36. ~~(TS//SI//NF)~~ In August 2007, Congress enacted the Protect America Act (PAA),
27 which carved out of the FISA definition of "electronic surveillance" a surveillance directed at a
28 person reasonably believed to be located outside the United States and authorized the Attorney
General and the Director of National Intelligence to jointly authorize the acquisition of foreign

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

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

1 intelligence information concerning persons reasonably believed to be located outside the United
2 States. The Foreign Telephone and E-mail Order was not renewed after the PAA was enacted.
3 Pursuant to applicable minimization procedures, the NSA was only authorized to retain
4 communications acquired pursuant to PAA certifications for five years. Subject to limited
5 exceptions, communications identified as domestic communications were to be promptly
6 destroyed. All NSA intelligence reports utilizing the content of communications intercepted
7 under PAA authority are currently retained permanently. The PAA expired on February 16,
8 2008 and, on July 11, 2008, the Foreign Intelligence Surveillance Act Amendments Act of 2008
9 (FAA) was signed into law.

10 37. (U) Section 702 of FISA, enacted by the FAA, created new statutory authority and
11 procedures permitting the targeting of non-United States persons reasonably believed to be
12 outside of the United States without individual FISC orders through directives issued to
13 electronic communication service providers by the Director of National Intelligence and the
14 Attorney General. Pursuant to the FISC-approved (and mandated) minimization procedures in
15 effect from August 2008 until October 2011, the NSA was only authorized to retain raw,
16 unminimized communications acquired pursuant to § 702 certifications for five years. Subject to
17 limited exceptions, domestic communications were to be destroyed upon recognition.

18 38. (U) On October 3, 2011, the FISC found certain aspects of NSA's § 702
19 minimization procedures to be inconsistent with certain statutory and constitutional
20 requirements, including the retention of certain information acquired by NSA. Accordingly,
21 NSA corrected the deficiencies identified by the FISC which, on November 30, 2011, found the
22 retention provisions of NSA's amended minimization procedures to comply with both § 702 and
23 the Fourth Amendment. The current NSA § 702 minimization procedures, which are in effect
24 today, authorize NSA to retain telephony and certain Internet communications no longer than
25 five years from the expiration date of the certification authorizing the collection. With respect to
26 the retention of Internet transactions acquired via NSA's "upstream" techniques, such
27 information must also be destroyed within two years of the expiration of the certification unless a
28 limited exception applies. Further, any Internet transactions acquired through NSA's upstream
collection techniques prior to October 31, 2011 will be destroyed upon recognition. Foreign

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


Approved for public release May 5, 2014

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

1 communications of or concerning United States persons collected in the course of an acquisition
2 authorized under § 702 may be retained pursuant to certain, specified exceptions. Finally,
3 subject to limited exceptions, domestic communications acquired pursuant to FAA 702 are to be
4 destroyed upon recognition. All NSA intelligence reports utilizing the content of intercepted
5 communications obtained under § 702 are preserved permanently.

6
7 I declare under penalty of perjury that the foregoing is true and correct.

8 Executed on: March 17, 2014

9 
10 Teresa H. Shea

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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