APPEAL,JURY,PROSE−NP,STAYED,TYPE−L

U.S. District Court
District of Columbia (Washington, DC)
CIVIL DOCKET FOR CASE #: 1:13−cv−00851−RJL

KLAYMAN v. OBAMA et al
Assigned to: Judge Richard J. Leon
Demand: $8,000,000
Cases: 1:14−cv−00092−RJL
1:11−cv−02214−RCL
1:14−cv−00262−RJL
1:15−cv−01353−RJL
1:13−cv−00881−RJL
1:14−cv−01431−RJL
Case in other court: 14−05004
14−05016
USCA, 14−05209
Cause: 28:1331 Fed. Question

Date Filed: 06/06/2013
Jury Demand: Plaintiff
Nature of Suit: 440 Civil Rights: Other
Jurisdiction: Federal Question

Plaintiff

LARRY E. KLAYMAN

represented by **LARRY E. KLAYMAN**
PRO SE

Larry E. Klayman
LAW OFFICES OF LARRY KLAYMAN
2020 Pennsylvania Avenue, NW
Suite 345
Washington, DC 20006
(310) 595−0800
Fax: (310) 275−3276
Email: leklayman@gmail.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

CHARLES STRANGE

represented by **Larry E. Klayman**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

MARY ANN STRANGE
on behalf of themselves and all others similarly situated

represented by **Larry E. Klayman**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

V.

Defendant

BARACK OBAMA

represented by

Bryan Scott Dearinger
U.S. DEPARTMENT OF JUSTICE
P.O. Box 883
Washington, DC 20044
(202) 514−3489
Fax: (202) 616−8202
Email: bryan.dearinger@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

James J. Gilligan
U.S. DEPARTMENT OF JUSTICE
CIVIL DIVISION, FEDERAL PROGRAMS BRANCH
20 Massachusetts Avenue, NW
Room 5138
Washington, DC 20001
(202) 514−3358
Fax: (202) 616−8470
Email: james.gilligan@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

James R. Whitman
U.S. DEPARTMENT OF JUSTICE
P.O. Box 7146
Washington, DC 20044
(202) 616−4169
Fax: 202−616−4314
Email: james.whitman@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Marcia Berman
UNITED STATES DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Room 7132
Washington, DC 20530
(202) 514−2205
Fax: (202) 616−8470
Email: marcia.berman@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
U.S. DEPARTMENT OF JUSTICE
Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, DC 20044

(202) 305−7919
Fax: (202) 616−8470
Email: rodney.patton@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia A. Berman
U.S. DEPARTMENT OF JUSTICE
Civil Division
20 Massachusetts Avenue, NW
Washington, DC 20001
(202) 616−8480
Fax: (202) 307−0442
Email: julia.berman@usdoj.gov
ATTORNEY TO BE NOTICED

Defendant

ERIC H. HOLDER, JR. represented by

Bryan Scott Dearinger
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

James J. Gilligan
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

James R. Whitman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Marcia Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia A. Berman
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

KEITH B. ALEXANDER represented by

Bryan Scott Dearinger
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

James J. Gilligan
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

James R. Whitman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Marcia Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia A. Berman
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

LOWELL C. MCADAMS
TERMINATED: 01/24/2014

represented by **Brian M. Boynton**
OFFICE OF BRIAN M. BOYNTON
4747 Fulton Stree, N.W.
Washington, DC 20007
(202) 329−1938
Email: brian_boynton@yahoo.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Randolph D. Moss
6116 Broad Street
Bethesda, MD 20816
(240) 988−4361
Email: randolph.moss@comcast.net
TERMINATED: 01/24/2014
LEAD ATTORNEY

Defendant

ROGER VINSON

represented by **James R. Whitman**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

represented by

VERIZON COMMUNICATIONS *TERMINATED: 01/24/2014*		**Brian M. Boynton** (See above for address) *LEAD ATTORNEY* *ATTORNEY TO BE NOTICED* **Randolph D. Moss** (See above for address) *TERMINATED: 01/24/2014* *LEAD ATTORNEY*
Defendant		
NATIONAL SECURITY AGENCY	represented by	**Bryan Scott Dearinger** (See above for address) *LEAD ATTORNEY* *ATTORNEY TO BE NOTICED* **James J. Gilligan** (See above for address) *LEAD ATTORNEY* *ATTORNEY TO BE NOTICED* **James R. Whitman** (See above for address) *LEAD ATTORNEY* *ATTORNEY TO BE NOTICED* **Marcia Berman** (See above for address) *LEAD ATTORNEY* *ATTORNEY TO BE NOTICED* **Rodney Patton** (See above for address) *LEAD ATTORNEY* *ATTORNEY TO BE NOTICED* **Julia A. Berman** (See above for address) *ATTORNEY TO BE NOTICED*
Defendant		
U.S. DEPARTMENT OF JUSTICE	represented by	**Bryan Scott Dearinger** (See above for address) *LEAD ATTORNEY* *ATTORNEY TO BE NOTICED* **James J. Gilligan** (See above for address) *LEAD ATTORNEY* *ATTORNEY TO BE NOTICED*

James R. Whitman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Marcia Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia A. Berman
(See above for address)
ATTORNEY TO BE NOTICED

Movant

DAVID ANDREW CHRISTENSON
TERMINATED: 07/30/2014

represented by **DAVID ANDREW CHRISTENSON**
P.O. Box 9063
Miramar Beach, FL 32550
PRO SE

Movant

TIMOTHY DEMITRI BROWN
TERMINATED: 07/30/2014

represented by **TIMOTHY DEMITRI BROWN**
R10979−035
FLORENCE ADMAX
U.S. PENITENTIARY
Inmate Mail/Parcels
PO BOX 8500
FLORENCE, CO 81226
PRO SE

Movant

FREDERICK BANKS

represented by **FREDERICK BANKS**
R05711−068
NEOCC
2240 Hubbard Road
Youngstown, OH 44505
PRO SE

Date Filed	#	Page	Docket Text
06/06/2013	1		COMPLAINT against All Defendants with Jury Demand (Filing fee $ 400 receipt number 0090−3352655) filed by LARRY E. KLAYMAN. (Attachments: # 1 Civil Cover Sheet, # 2 Summons Mr. Obama, # 3 Summons Mr. Holder, # 4 Summons Mr. Alexander, # 5 Summons Mr. McAdam, # 6 Summons Mr. Vinson, # 7 Summons Verizon Communications, # 8 Summons

			Department of Justice, # 9 Summons National Security Agency)(Klayman, Larry) (Entered: 06/06/2013)
06/06/2013			Case Assigned to Judge Richard J. Leon. (ls,) (Entered: 06/07/2013)
06/07/2013	2		ELECTRONIC SUMMONS (8) Issued as to KEITH B. ALEXANDER, ERIC HIMPTON HOLDER, JR, LOWELL C. MCADAMS, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE, VERIZON COMMUNICATIONS, ROGER VINSON (Attachments: # 1 Summons, # 2 Summons, # 3 Summons, # 4 Summons, # 5 Summons, # 6 Memorandum in Support, # 7 Summons, # 8 Consent Notice)(ls,) (Entered: 06/07/2013)
06/07/2013	3		CIVIL COVER SHEET *(Amended)* by LARRY E. KLAYMAN re 1 Complaint, filed by LARRY E. KLAYMAN. Related document: 1 Complaint, filed by LARRY E. KLAYMAN.(Klayman, Larry) (Entered: 06/07/2013)
06/09/2013	4		AMENDED COMPLAINT against All Defendants with Jury Demand filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE.(Klayman, Larry) Modified filers on 6/10/2013 (znmw,). (Entered: 06/09/2013)
06/12/2013	5		NOTICE of Appearance by James R. Whitman on behalf of NATIONAL SECURITY AGENCY, U.S. DEPARTMENT OF JUSTICE (Whitman, James) (Entered: 06/12/2013)
06/12/2013	6		STANDING ORDER. Signed by Judge Richard J. Leon on 6/12/13. (lcrjl1) (Entered: 06/12/2013)
09/30/2013	7		MOTION for Extension of Time to *Certify Class Action* by LARRY E. KLAYMAN (Attachments: # 1 Text of Proposed Order)(Klayman, Larry) (Entered: 09/30/2013)
10/10/2013	8		MOTION for Extension of Time to File Answer by VERIZON COMMUNICATIONS (Attachments: # 1 Text of Proposed Order)(Moss, Randolph) (Entered: 10/10/2013)
10/11/2013	9		Corporate Disclosure Statement by VERIZON COMMUNICATIONS. (Moss, Randolph) (Entered: 10/11/2013)
10/11/2013	10		MOTION to Stay *(Government Defendants' Motion for a Stay of Deadline to Respond to the Complaint in Light of Lapse in Appropriations)* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 10/11/2013)
10/14/2013	11		Memorandum in opposition to re 7 MOTION for Extension of Time to *Certify Class Action* filed by VERIZON COMMUNICATIONS. (Attachments: # 1 Text of Proposed Order)(Moss, Randolph) (Entered: 10/14/2013)
10/15/2013			MINUTE ORDER granting 8 Motion for Extension of Time to Respond re 4 Amended Complaint. It is hereby ORDERED that the motion is GRANTED and defendant Verizon Communications Inc. has up to and including 12/2/2013 to respond to plaintiffs' amended complaint. Signed by Judge Richard J. Leon on 10/15/13. (lcrjl1,) (Entered: 10/15/2013)

10/15/2013			Set/Reset Deadlines: Response due by 12/2/2013. (tb,) (Entered: 10/16/2013)
10/17/2013	12		MOTION for Extension of Time to File Answer by LOWELL C. MCADAMS (Attachments: # 1 Text of Proposed Order)(Moss, Randolph) (Entered: 10/17/2013)
10/20/2013			MINUTE ORDER granting 12 Motion for Extension of Time to Respond re 4 Amended Complaint. It is hereby ORDERED that the motion is GRANTED and defendant LOWELL C. MCADAMS shall have up to and including 12/2/2013 to respond to plaintiffs' amended complaint. Signed by Judge Richard J. Leon on 10/20/2013. (lcrjl1,) (Entered: 10/20/2013)
10/21/2013			Set/Reset Deadlines: Defendant LOWELL C. MCADAMS response to the amended complaint is due by 12/2/2013. (jth) (Entered: 10/21/2013)
10/29/2013	13		MOTION for Preliminary Injunction by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Memorandum in Support, # 2 Exhibit 1 −− Affidavit of Larry Klayman, # 3 Exhibit 2 −− Affidavit of Charles Strange, # 4 Text of Proposed Order)(Klayman, Larry) (Entered: 10/29/2013)
10/29/2013			Minute Order. Scheduling Conference set for 10/31/2013 at 03:45 PM in Courtroom 18 before Judge Richard J. Leon. (lcrjl1,) (Entered: 10/29/2013)
10/29/2013	14		MOTION for Extension of Time to *Certify Class Action* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Text of Proposed Order)(Klayman, Larry) (Entered: 10/29/2013)
10/30/2013	15		MOTION For Leave of Court To Take FRCP Rule 30(B)(6) Deposition re 13 MOTION for Preliminary Injunction by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Government's Opposition to ACLU's Motion for Preliminary Injunction, # 2 Text of Proposed Order)(Klayman, Larry) (Entered: 10/30/2013)
10/30/2013	16		MOTION for Extension of Time to File Response/Reply as to 13 MOTION for Preliminary Injunction by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 10/30/2013)
10/30/2013	17		MOTION For Leave of Court to Appear Telephonically re Set Hearings by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Text of Proposed Order)(Klayman, Larry) (Entered: 10/30/2013)
10/30/2013	18		NOTICE *of Consent* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE re 17 MOTION For Leave of Court to Appear Telephonically re Set Hearings (Klayman, Larry) (Entered: 10/30/2013)
10/30/2013			MINUTE ORDER denying 17 Motion for Leave to Appear Telephonically. It is hereby ORDERED that plaintiffs' Motion for Leave to Appear Telephonically at the Scheduling Conference set for 10/31/2013 at 03:45 PM in Courtroom 18 before Judge Richard J. Leon is DENIED. Signed by Judge Richard J. Leon on 10/30/2013. (lcrjl1,) (Entered: 10/30/2013)
10/30/2013	19		

			MOTION to Continue *Status Conference Concerning Preliminary Injunction* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Text of Proposed Order)(Klayman, Larry) (Entered: 10/30/2013)
10/31/2013	20		Memorandum in opposition to re 14 MOTION for Extension of Time to *Certify Class Action* filed by LOWELL C. MCADAMS, VERIZON COMMUNICATIONS. (Attachments: # 1 Text of Proposed Order)(Boynton, Brian) (Entered: 10/31/2013)
10/31/2013			MINUTE ORDER denying 19 Motion to Continue. It is hereby ORDERED that plaintiffs' Motion to Continue the Scheduling Conference set for 10/31/2013 at 03:45 PM in Courtroom 18 before Judge Richard J. Leon is DENIED. Signed by Judge Richard J. Leon on 10/31/2013. (lcrjl1,) (Entered: 10/31/2013)
10/31/2013	21		MOTION for Reconsideration re Order on Motion to Continue, by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1, # 2 Text of Proposed Order)(Klayman, Larry) (Entered: 10/31/2013)
10/31/2013			MINUTE ORDER denying 21 Motion for Reconsideration. It is hereby ORDERED that Plaintiffs' Motion for Reconsideration of 19 Plaintiffs' Motion to Continue is DENIED. Signed by Judge Richard J. Leon on 10/31/2013. (lcrjl1,) (Entered: 10/31/2013)
10/31/2013			Minute Entry: Status Conference held on 10/31/2013 before Judge Richard J. Leon: Plaintiff counsel not present. Transcript of the hearing will be sent to plaintiff counsel. Response to Preliminary Injunction Motion due by 11/11/2013. Reply due by 11/14/2013. Oral arugment set for 11/18/2013 at 11:30 AM in Courtroom 18 before Judge Richard J. Leon. (Court Reporter Patty Gels) (tb,) (Entered: 11/01/2013)
11/01/2013	22		MOTION For Leave to File Supplemental Declaration re 13 MOTION for Preliminary Injunction by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Declaration of Professor Edward Felten, # 2 Exhibit 2 −− Washington Post Article, # 3 Text of Proposed Order)(Klayman, Larry) (Entered: 11/01/2013)
11/03/2013			MINUTE ORDER denying 10 Government Defendants' Motion for Stay of Deadline to Respond to Complaint in Light of Lapse in Appropriations. It is hereby ORDERED that the motion is DENIED. Signed by Judge Richard J. Leon on 11/3/2013. (lcrjl1,) (Entered: 11/03/2013)
11/06/2013			MINUTE ORDER granting 22 MOTION for Leave to File Supplemental Declaration. It is hereby ORDERED that plaintiffs' motion is GRANTED and the Declaration of Professor Edward W. Felten is accepted for filing. Signed by Judge Richard J. Leon on 11/6/2013. (lcrjl1,) (Entered: 11/06/2013)
11/06/2013	23		Supplemental Declaration re 13 MOTION for Preliminary Injunction by LARRY E. KLAYMAN. (znmw,) (Entered: 11/08/2013)
11/08/2013	24		Unopposed MOTION for Leave to File Excess Pages *In The Combined Opposition to Plaintiffs' Preliminary Injunction Motions* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY,

			BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Patton, Rodney) (Entered: 11/08/2013)
11/08/2013			MINUTE ORDER granting 24 Motion for Leave to File Excess Pages. It is hereby ORDERED that the motion is GRANTED and that the page limit for Government Defendants' combined opposition is enlarged from 45 to 65 pages. Signed by Judge Richard J. Leon on 11/8/2013. (lcrjl1,) (Entered: 11/08/2013)
11/12/2013	25		Memorandum in opposition to re 13 MOTION for Preliminary Injunction filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Declaration (Declaration of James J. Gilligan), # 2 Exhibit (Exhibit A), # 3 Exhibit (Exhibit B), # 4 Exhibit (Exhibit C), # 5 Exhibit (Exhibit D), # 6 Exhibit (Exhibit E), # 7 Exhibit (Exhibit F), # 8 Exhibit (Exhibit G), # 9 Exhibit (Exhibit H), # 10 Exhibit (Exhibit I), # 11 Exhibit (Exhibit J), # 12 Exhibit (Exhibit K), # 13 Exhibit (Exhibit L), # 14 Exhibit (Exhibit M), # 15 Exhibit (Exhibit N), # 16 Exhibit (Exhibit O), # 17 Exhibit (Exhibit P), # 18 Exhibit (Exhibit Q), # 19 Exhibit (Exhibit R), # 20 Exhibit (Exhibit S), # 21 Exhibit (Exhibit T), # 22 Text of Proposed Order)(Gilligan, James) (Entered: 11/12/2013)
11/12/2013	26		Unopposed MOTION For Leave To File Reply Brief With Extended Pages And A Supplemental Declaration by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Supplemental Declaration of Professor Edward Felton, # 2 Text of Proposed Order)(Klayman, Larry) (Entered: 11/12/2013)
11/12/2013			MINUTE ORDER granting 26 Motion for Leave to File Reply Brief with Extended Pages and a Supplemental Declaration. It is hereby ORDERED that the motion is GRANTED and that the page limit for Plaintiffs' reply is enlarged from 25 to 50 pages; and it is further ordered that the Supplemental Declaration of Professor Edward W. Felten is accepted for filing. Signed by Judge Richard J. Leon on 11/12/2013. (lcrjl1,) (Entered: 11/12/2013)
11/12/2013	27		MOTION for Extension of Time to Certify Class Action by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Text of Proposed Order)(Klayman, Larry) (Entered: 11/12/2013)
11/12/2013	28		Supplemental Declaration of Dr. Edward Felton by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (jf,) (Entered: 11/13/2013)
11/13/2013	29		MOTION for Extension of Time to File Response/Reply *to Plaintiffs' Two Preliminary Injunction Motions* by KEITH B. ALEXANDER, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Patton, Rodney) (Entered: 11/13/2013)
11/13/2013	30		Memorandum in opposition to re 27 MOTION for Extension of Time to Certify Class Action filed by LOWELL C. MCADAMS, VERIZON COMMUNICATIONS. (Attachments: # 1 Text of Proposed Order)(Boynton, Brian) (Entered: 11/13/2013)
11/14/2013	31		REPLY to opposition to motion re 13 MOTION for Preliminary Injunction filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN

			STRANGE. (Attachments: # 1 Exhibit 1 − Letter to Senator Grassley, # 2 Exhibit 2 −− Supplemental Affidavit of Larry Klayman, # 3 Exhibit 3 −− NSA Touhy Request, # 4 Text of Proposed Order)(Klayman, Larry) (Entered: 11/14/2013)
11/15/2013			MINUTE ORDER granting, nunc pro tunc, 29 Government Defendants' Motion for Extension of Time to File Combined Opposition to Plaintiffs' Two Motions for Preliminary Injunctions. Signed by Judge Richard J. Leon on 11/15/2013. (lcrjl1,) (Entered: 11/15/2013)
11/15/2013	32		NOTICE *of Filing of Amended Proposed Order* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE re 13 MOTION for Preliminary Injunction (Attachments: # 1 Certificate of Service)(Klayman, Larry) (Entered: 11/15/2013)
11/17/2013	33		MOTION to Amend/Correct 4 Amended Complaint by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Second Amended Complaint, # 2 Text of Proposed Order)(Klayman, Larry) (Entered: 11/17/2013)
11/17/2013	34		MOTION for Leave to File Supplemental Affidavit re 13 MOTION for Preliminary Injunction by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Affidavit of David Siler, # 2 Text of Proposed Order)(Klayman, Larry) (Entered: 11/17/2013)
11/18/2013			Minute Entry: Preliminary Injunction Heaing held on 11/18/2013 before Judge Richard J. Leon: Motion heard and taken under advisement. Supplemental briefs are due by COB on 11/26/2013. Defendant's response to plaintiffs' 33 Motion for Leave to File Amended Complaint due by 11/22/2013. (Court Reporter Patty Gels) (tb,) (Entered: 11/18/2013)
11/21/2013	35		MOTION for Extension of Time to *Respond to the Complaint* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 11/21/2013)
11/21/2013	36		Memorandum in opposition to re 33 MOTION to Amend/Correct 4 Amended Complaint filed by LOWELL C. MCADAMS, VERIZON COMMUNICATIONS. (Attachments: # 1 Text of Proposed Order)(Boynton, Brian) (Entered: 11/21/2013)
11/23/2013			MINUTE ORDER granting 33 Plaintiffs' Motion for Leave to File Second Amended Complaint. It is hereby ORDERED that the motion is GRANTED and that Plaintiffs' Second Amended Complaint is accepted for filing. Signed by Judge Richard J. Leon on 11/23/2013. (lcrjl1,) (Entered: 11/23/2013)
11/23/2013			MINUTE ORDER granting 34 Plaintiffs' Motion for Leave to File Supplemental Affidavit. It is hereby ORDERED that the motion is GRANTED and that the Supplemental Affidavit of David M. Siler is accepted for filing. Signed by Judge Richard J. Leon on 11/23/2013. (lcrjl1,) (Entered: 11/23/2013)
11/23/2013			MINUTE ORDER granting 35 Motion for Extension of Time to Respond to Complaint. It is hereby ORDERED that the motion is GRANTED, and it is

			further ORDERED that the Government Defendants and the Verizon Defendants shall have up to and including 12/16/2013 to file their responses to the complaint. Signed by Judge Richard J. Leon on 11/23/2013. (lcrjl1,) (Entered: 11/23/2013)
11/23/2013	37		SECOND AMENDED COMPLAINT against KEITH B. ALEXANDER, ERIC H. HOLDER, JR, LOWELL C. MCADAMS, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE, VERIZON COMMUNICATIONS, ROGER VINSON filed by MARY ANN STRANGE, LARRY E. KLAYMAN, CHARLES STRANGE.(znmw,) (Entered: 11/25/2013)
11/23/2013	38		AFFIDAVIT of David M. Siler by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (znmw,) (Entered: 11/25/2013)
11/25/2013	39		NOTICE *of Filing of Transcript* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Transcript of ACLU v. Clapper Proceeding)(Klayman, Larry) (Entered: 11/25/2013)
11/25/2013	40		MOTION for Extension of Time to *Certify Class Action* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Text of Proposed Order)(Klayman, Larry) (Entered: 11/25/2013)
11/26/2013			Set/Reset Deadlines: Answer due by 12/16/2013. (tb,) (Entered: 11/26/2013)
11/26/2013	41		TRANSCRIPT OF PROCEEDINGS before Judge Richard J. Leon held on 11/18/13; Date of Issuance:11/26/13. Court Reporter/Transcriber Patty Gels, Telephone number 2023543236, Court Reporter Email Address : Patty_Gels@dcd.uscourts.gov.<P></P>For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi−page, condensed, CD or ASCII) may be purchased from the court reporter.<P>**NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty−one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at ww.dcd.uscourts.gov.<P></P> Redaction Request due 12/17/2013. Redacted Transcript Deadline set for 12/27/2013. Release of Transcript Restriction set for 2/24/2014.(Gels, Patty) (Entered: 11/26/2013)
11/26/2013	42		NOTICE *of Filing of Bench Briefs* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Bench Brief on Jurisdiction, # 2 Exhibit 2 −− Bench Brief on Admissibility of Snowden Statements)(Klayman, Larry) (Entered: 11/26/2013)
11/26/2013	43		SUPPLEMENTAL MEMORANDUM to re 13 MOTION for Preliminary Injunction *(Government Defendants' Supplemental Brief in Opposition to Plaintiffs' Motions for Preliminary Injunctions)* filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Exhibit A)(Gilligan, James) (Entered: 11/26/2013)

11/26/2013	44		MEMORANDUM by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Attachments: # 1 Exhibit 1 −− Binder Part 1, # 2 Exhibit 1 −− Binder Part 2, # 3 Exhibit 2 −− Gov't Opposition in In Re Epic)(Klayman, Larry) (Entered: 11/26/2013)
11/30/2013	45		Memorandum in opposition to re 40 MOTION for Extension of Time to *Certify Class Action* filed by LOWELL C. MCADAMS, VERIZON COMMUNICATIONS. (Attachments: # 1 Text of Proposed Order)(Boynton, Brian) (Entered: 11/30/2013)
12/02/2013	46		MOTION for Leave to Supplement the Record by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1, # 2 Text of Proposed Order)(Klayman, Larry) (Entered: 12/02/2013)
12/04/2013	47		Memorandum in opposition to re 46 MOTION for Leave to Supplement the Record filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 12/04/2013)
12/16/2013	48		MEMORANDUM AND OPINION. Signed by Judge Richard J. Leon on 12/16/13. (tb,) (Entered: 12/16/2013)
12/16/2013	49		ORDER: For the reasons set forth in the Memorandum Opinion entered this date, it is hereby ordered that 13 Motion for Preliminary Injunction is GRANTED as to plaintiff's Larry Klayman and Charles Strange and DENIED as to plaintiff Mary Ann Strange; it is further ordered that the Motion for Preliminary Injunction in Klayman v. Obama in Civil Action 13−881 is DENIED; and it is further ordered that this Order is STAYED pending appeal. Signed by Judge Richard J. Leon on 12/16/13. (tb,) (Entered: 12/16/2013)
12/16/2013	50		NOTICE of Appearance by Marcia Berman on behalf of KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Berman, Marcia) (Entered: 12/16/2013)
12/16/2013	51		MOTION for Extension of Time to *Respond to Plaintiffs' Amended Complaints in Light of Memorandum Opinion Issued Today* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Berman, Marcia) (Entered: 12/16/2013)
12/16/2013	52		MOTION to Dismiss *or, in the Alternative for Summary Judgment, Regarding Plaintiffs' Claims Against the Verizon Defendants* by U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Memorandum in Support, # 2 Text of Proposed Order, # 3 Exhibit, # 4 Exhibit, # 5 Exhibit, # 6 Exhibit)(Patton, Rodney). Added MOTION for Summary Judgment on 12/17/2013 (znmw,). (Entered: 12/16/2013)
12/16/2013	53		NOTICE *of Lodging of Classified Certification and Declaration of the Deputy Attorney General for in Camera and Ex Parte Review* by U.S. DEPARTMENT OF JUSTICE re 52 MOTION to Dismiss *or, in the Alternative for Summary Judgment, Regarding Plaintiffs' Claims Against the Verizon Defendants* (Patton, Rodney) (Entered: 12/16/2013)

12/16/2013	54		NOTICE *of Lodging of Classified Declaration of Acting Deputy Director of the National Security Agency for In Camera and Ex Parte Review* by U.S. DEPARTMENT OF JUSTICE re 52 MOTION to Dismiss *or, in the Alternative for Summary Judgment, Regarding Plaintiffs' Claims Against the Verizon Defendants* (Patton, Rodney) (Entered: 12/16/2013)
12/16/2013	55		MOTION to Dismiss *Plaintiffs' Second Amended Complaint* by LOWELL C. MCADAMS, VERIZON COMMUNICATIONS (Attachments: # 1 Declaration of Jane A. Schapker, # 2 Text of Proposed Order)(Moss, Randolph) (Entered: 12/16/2013)
12/16/2013	56		ENTERED IN ERROR.....MOTION for Extension of Time by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE, DEPARTMENT OF JUSTICE OF THE UNITED STATES (Attachments: # 1 Text of Proposed Order)(rdj) Modified on 12/17/2013 (rdj). (Entered: 12/17/2013)
12/17/2013	57		ERRATA *Attaching Corrected Exhibit D* by U.S. DEPARTMENT OF JUSTICE 52 MOTION to Dismiss *or, in the Alternative for Summary Judgment, Regarding Plaintiffs' Claims Against the Verizon Defendants* MOTION for Summary Judgment filed by U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Exhibit)(Patton, Rodney) (Entered: 12/17/2013)
12/17/2013	58		ERRATA *Substituting Corrected Version of Exhibit D* by U.S. DEPARTMENT OF JUSTICE 52 MOTION to Dismiss *or, in the Alternative for Summary Judgment, Regarding Plaintiffs' Claims Against the Verizon Defendants* MOTION for Summary Judgment filed by U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Exhibit)(Patton, Rodney) (Entered: 12/17/2013)
12/17/2013	59		TRANSCRIPT OF PROCEEDINGS before Judge Richard J. Leon held on 10/31/13; Date of Issuance:12/17/13. Court Reporter/Transcriber Patty Gels, Telephone number 202−354−3236, Court Reporter Email Address : Patty_Gels@dcd.uscourts.gov.<P></P>For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi−page, condensed, CD or ASCII) may be purchased from the court reporter.<P>**NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty−one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at ww.dcd.uscourts.gov.<P></P> Redaction Request due 1/7/2014. Redacted Transcript Deadline set for 1/17/2014. Release of Transcript Restriction set for 3/17/2014.(Gels, Patty) (Entered: 12/17/2013)
12/17/2013	60		MOTION for Extension of Time to *Certify Class Action* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Text of Proposed Order)(Klayman, Larry) (Entered: 12/17/2013)
12/18/2013	61		

			Memorandum in opposition to re 60 MOTION for Extension of Time to *Certify Class Action* filed by LOWELL C. MCADAMS, VERIZON COMMUNICATIONS. (Attachments: # 1 Text of Proposed Order)(Boynton, Brian) (Entered: 12/18/2013)
12/24/2013	62		MOTION for Extension of Time to File Response/Reply as to 55 MOTION to Dismiss *Plaintiffs' Second Amended Complaint*, 52 MOTION to Dismiss *or, in the Alternative for Summary Judgment, Regarding Plaintiffs' Claims Against the Verizon Defendants* MOTION for Summary Judgment by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Text of Proposed Order)(Klayman, Larry) (Entered: 12/24/2013)
12/30/2013	63		MOTION Status Conference by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Fox News article, # 2 Text of Proposed Order)(Klayman, Larry) (Entered: 12/30/2013)
01/03/2014	64		NOTICE OF APPEAL TO DC CIRCUIT COURT as to 48 Memorandum & Opinion, 49 Order on Motion for Preliminary Injunction, by ERIC H. HOLDER, JR, U.S. DEPARTMENT OF JUSTICE, BARACK HUSSEIN OBAMA, II, NATIONAL SECURITY AGENCY, KEITH B. ALEXANDER. Fee Status: No Fee Paid. Parties have been notified. (Berman, Marcia) (Entered: 01/03/2014)
01/06/2014	65		Transmission of the Notice of Appeal, Order Appealed, and Docket Sheet to US Court of Appeals. The Court of Appeals docketing fee was not paid because the fee was an Appeal by the Government re 64 Notice of Appeal to DC Circuit Court. (znmw,) (Entered: 01/06/2014)
01/08/2014	66		MOTION to Stay *Proceedings Against the Government Defendants Pending Appeal of Preliminary Injunction* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 01/08/2014)
01/10/2014			USCA Case Number 14−5004 for 64 Notice of Appeal to DC Circuit Court, filed by NATIONAL SECURITY AGENCY, KEITH B. ALEXANDER, U.S. DEPARTMENT OF JUSTICE, ERIC H. HOLDER, JR., BARACK HUSSEIN OBAMA, II. (jf,) (Entered: 01/10/2014)
01/10/2014	67		NOTICE OF CROSS APPEAL as to 48 Memorandum & Opinion, 49 Order on Motion for Preliminary Injunction, by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. Filing fee $ 505, receipt number 0090−3588427. Fee Status: Fee Paid. Parties have been notified. (Klayman, Larry) (Entered: 01/10/2014)
01/10/2014	68		MOTION to Dismiss *(The Government Defendants' Partial Motion To Dismiss and Memorandum in Support)* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 01/10/2014)
01/13/2014	69		Transmission of the Notice of Appeal, Order Appealed, and Docket Sheet to US Court of Appeals. The Court of Appeals fee was paid this date re 67 Notice of Cross Appeal,. (znmw,) (Entered: 01/13/2014)

01/15/2014	70		Memorandum in Opposition re 66 MOTION to Stay *Proceedings Against the Government Defendants Pending Appeal of Preliminary Injunction* filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Attachments: # 1 Exhibit 1 − Transcript of Oct. 31, 2013, # 2 Exhibit 2 − Transcript of Nov. 18, 2013)(Klayman, Larry) Modified event title on 1/16/2014 (znmw,). (Entered: 01/15/2014)
01/15/2014	71		NOTICE *Praecipe Regarding Class Actions* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Klayman, Larry) (Entered: 01/15/2014)
01/16/2014	72		MOTION for Extension of Time to File Response/Reply as to 55 MOTION to Dismiss *Plaintiffs' Second Amended Complaint*, 52 MOTION to Dismiss *or, in the Alternative for Summary Judgment, Regarding Plaintiffs' Claims Against the Verizon Defendants* MOTION for Summary Judgment by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Text of Proposed Order)(Klayman, Larry) (Entered: 01/16/2014)
01/21/2014			MINUTE ORDER granting, nunc pro tunc, 62 Motion for Extension of Time to File Response re 52 MOTION to Dismiss *or, in the Alternative for Summary Judgment, Regarding Plaintiffs' Claims Against the Verizon Defendants*, and 55 MOTION to Dismiss *Plaintiffs' Second Amended Complaint*. It is hereby ORDERED that the motion is GRANTED nunc pro tunc; and it is further ordered that plaintiffs' responses are due by 1/16/2014. Signed by Judge Richard J. Leon on 1/21/2014. (lcrjl1,) (Entered: 01/21/2014)
01/21/2014			MINUTE ORDER granting 72 Motion for Extension of Time to File Response re 52 MOTION to Dismiss *or, in the Alternative for Summary Judgment, Regarding Plaintiffs' Claims Against the Verizon Defendants*, and 55 MOTION to Dismiss *Plaintiffs' Second Amended Complaint*. It is hereby ORDERED that the motion is GRANTED; and it is further ORDERED that plaintiffs' responses are due by 1/30/2014, but further extensions on this motion will not be entertained. Signed by Judge Richard J. Leon on 1/21/2014. (lcrjl1,) (Entered: 01/21/2014)
01/21/2014			MINUTE ORDER denying as moot 15 Motion for Leave to Take Deposition. It is hereby ORDERED that the motion is DENIED as moot. Signed by Judge Richard J. Leon on 1/21/2014. (lcrjl1,) (Entered: 01/21/2014)
01/21/2014			MINUTE ORDER denying as moot 16 Government Defendants' Motion for Extension of Time to File Response to Plaintiffs' Motions for Preliminary Injunctions. It is hereby ORDERED that the motion is DENIED as moot. Signed by Judge Richard J. Leon on 1/21/2014. (lcrjl1,) (Entered: 01/21/2014)
01/21/2014			MINUTE ORDER denying 46 Motion for Leave to Supplement the Record. It is hereby ORDERED that the motion is DENIED. Signed by Judge Richard J. Leon on 1/21/2014. (lcrjl1,) (Entered: 01/21/2014)
01/22/2014			Set/Reset Hearings: Status Conference set for 2/3/2014 02:30 PM in Courtroom 18 before Judge Richard J. Leon. (tb,) (Entered: 01/22/2014)
01/23/2014			Set/Reset Deadlines: Response due by 1/30/2014. (tb,) (Entered: 01/23/2014)
01/23/2014			Set/Reset Deadlines: Response due by 1/16/2014. (tb,) (Entered: 01/23/2014)
01/23/2014	73		

			NOTICE of Voluntary Dismissal re Verizon Communications and Lowell C. McAdam (Klayman, Larry) (Entered: 01/23/2014)
01/24/2014			USCA Case Number 14−5016 for 67 Notice of Cross Appeal, filed by LARRY E. KLAYMAN, MARY ANN STRANGE, CHARLES STRANGE. (jf,) (Entered: 01/24/2014)
01/28/2014			MINUTE ORDER: At the status conference scheduled for 2/3/2014 at 2:30 PM, the Court will hear oral argument from the parties, including the Verizon Defendants, regarding whether 73 Plaintiffs' Notice of Voluntary Dismissal of Verizon Defendants without prejudice pursuant to Fed. R. Civ. P. 41(a)(1)(A) should be effective. Signed by Judge Richard J. Leon on 1/28/2014. (lcrjl1,) (Entered: 01/28/2014)
01/30/2014	74		RESPONSE re 68 MOTION to Dismiss *(The Government Defendants' Partial Motion To Dismiss and Memorandum in Support)* filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Klayman, Larry) (Entered: 01/30/2014)
01/31/2014	75		STIPULATION of Dismissal by LOWELL C. MCADAMS, VERIZON COMMUNICATIONS. (Boynton, Brian) (Entered: 01/31/2014)
02/03/2014			Minute Entry: Status Conference held on 2/3/2014 before Judge Richard J. Leon. Government Defendants' Partial Motion to Dismiss 68 DENIED as moot with respect to 13−cv−851. Government defendants' answer in 13−cv−851 is due 2/10/2014. (Court Reporter Patty Gels) (tb) Modified on 2/10/2014 (tb). (Entered: 02/04/2014)
02/05/2014	76		STRICKEN PURSUANT TO MINUTE ORDER FILED 2/7/2014.....AMENDED COMPLAINT *(Third Amended Complaint)* against KEITH B. ALEXANDER, ERIC H. HOLDER, JR, LOWELL C. MCADAMS, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE, ROGER VINSON with Jury Demand filed by MARY ANN STRANGE, LARRY E. KLAYMAN, CHARLES STRANGE.(Klayman, Larry) Modified on 2/10/2014 (znmw,). (Entered: 02/05/2014)
02/07/2014			MINUTE ORDER striking 76 Third Amended Complaint. It is hereby ORDERED that plaintiffs' Third Amended Complaint be stricken from the record. It is further ORDERED that plaintiffs shall re−file their amended complaint consistent with the Court's instructions at the February 3, 2014 status conference. Plaintiffs previously withdrew certain legal claims in their 74 Opposition to Government Defendants' Partial Motion to Dismiss, and based on that representation this Court denied as moot 68 Government Defendants' Partial Motion to Dismiss (with respect to 13−cv−851 only). Accordingly, amendments to plaintiffs' complaint shall not include the addition of new defendants, new facts, or new legal claims. SO ORDERED. Signed by Judge Richard J. Leon on 2/7/2014. (lcrjl1,) (Entered: 02/07/2014)
02/10/2014	77		AMENDED COMPLAINT *(Third Amended Complaint)* against KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE, ROGER VINSON with Jury Demand filed by MARY ANN STRANGE, LARRY E. KLAYMAN, CHARLES STRANGE.(Klayman, Larry) (Entered: 02/10/2014)

02/10/2014	78		Unopposed MOTION for Extension of Time to File Answer re 77 Amended Complaint, by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 02/10/2014)
02/10/2014			MINUTE ORDER granting 78 Unopposed Motion for an Extension of Time to File the Government Defendants' Answer in Klayman I. It is hereby ORDERED that the motion is GRANTED; and it is further ORDERED that the Government defendants' answer is due 2/14/2014. Signed by Judge Richard J. Leon on 2/10/2014. (lcrjl1,) (Entered: 02/10/2014)
02/10/2014			Set/Reset Deadlines: The Government Defendants' Answer to the Amended Complaint in (Klayman I) is due by 2/14/2014. (jth) (Entered: 02/10/2014)
02/10/2014			Set/Reset Deadlines: Answer due by 2/14/2014. (tb,) (Entered: 02/10/2014)
02/10/2014	79		MOTION to Supplement the Record by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Klayman, Larry) (Entered: 02/10/2014)
02/10/2014	80		NOTICE *of Filing of Exhibit 1* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE re 79 MOTION to Supplement the Record (Klayman, Larry) (Entered: 02/10/2014)
02/10/2014	81		NOTICE *of Filing of Proposed Order* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE re 79 MOTION to Supplement the Record (Klayman, Larry) (Entered: 02/10/2014)
02/10/2014	82		REPLY to opposition to motion re 68 MOTION to Dismiss *(The Government Defendants' Partial Motion To Dismiss and Memorandum in Support)* filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Gilligan, James) (Entered: 02/10/2014)
02/14/2014	83		ANSWER to 77 Amended Complaint, *(Government Defendants' Answer to Plaintiffs' Third Amended Complaint)* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. Related document: 77 Amended Complaint, filed by LARRY E. KLAYMAN, MARY ANN STRANGE, CHARLES STRANGE.(Gilligan, James) (Entered: 02/14/2014)
02/20/2014	84		TRANSCRIPT OF PROCEEDINGS before Judge Richard J. Leon held on 2/3/14; Date of Issuance:2/20/14. Court Reporter/Transcriber Patty Gels, Telephone number 202−354−3236, Court Reporter Email Address : Patty_Gels@dcd.uscourts.gov.<P></P>For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi−page, condensed, CD or ASCII) may be purchased from the court reporter.<P>**NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty−one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at

			ww.dcd.uscourts.gov.<P></P> Redaction Request due 3/13/2014. Redacted Transcript Deadline set for 3/23/2014. Release of Transcript Restriction set for 5/21/2014.(Gels, Patty) (Entered: 02/20/2014)
02/20/2014	85		MOTION For Entry Of Default And To Strike Government Defendants Answer To Plaintiffs Third Amended Complaint re 83 Answer to Amended Complaint, by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Affidavit Demonstrating Proper Service, # 2 Text of Proposed Order)(Klayman, Larry) (Entered: 02/20/2014)
02/25/2014	86		NOTICE *Praecipe* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Reply filed by the Government Defendants)(Klayman, Larry) (Entered: 02/25/2014)
02/26/2014	93		MOTION to Join, MOTION to Intervene by DAVID ANDREW CHRISTENSON (jf,). (Entered: 03/07/2014)
02/27/2014	87		Memorandum in opposition to re 79 MOTION to Supplement the Record filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Text of Proposed Order)(Dearinger, Bryan) (Entered: 02/27/2014)
02/28/2014	88		Memorandum in opposition to re 85 MOTION For Entry Of Default And To Strike Government Defendants Answer To Plaintiffs Third Amended Complaint re 83 Answer to Amended Complaint, filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, BARACK HUSSEIN OBAMA, II, ROGER VINSON. (Attachments: # 1 Exhibit Transcript of proceedings)(Whitman, James) (Entered: 02/28/2014)
03/04/2014	89		REPLY to opposition to motion re 79 MOTION to Supplement the Record filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Klayman, Larry) (Entered: 03/04/2014)
03/05/2014	90		LEAVE TO FILE DENIED− John Stewart Stritzinger, Motion For Pro Hac Vice, Motion For Electronic Filing, and Motion to Modify Judgment or Motion for Teleconference Hearing Prior to Appeal This document is unavailable as the Court denied its filing. "Leave to file Denied". Signed by Judge Richard J. Leon on 3/5/2014. (zrdj,) (Entered: 03/05/2014)
03/05/2014	91		LEAVE TO FILE DENIED− John Stewart Stritzinger, Motion to Seal This document is unavailable as the Court denied its filing. "Leave to file Denied". Signed by Judge Richard J. Leon on 3/5/2014. (zrdj) (Entered: 03/05/2014)
03/05/2014	92		REPLY to opposition to motion re 85 MOTION For Entry Of Default And To Strike Government Defendants Answer To Plaintiffs Third Amended Complaint re 83 Answer to Amended Complaint, filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Klayman, Larry) (Entered: 03/05/2014)
03/06/2014	95		MOTION to Join and for Leave by TIMOTHY DEMITRI BROWN (jf,) (Entered: 03/10/2014)
03/07/2014	94		NOTICE *Regarding Order of the Foreign Intelligence Surveillance Court* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF

			JUSTICE (Attachments: # 1 Exhibit 1, # 2 Exhibit 2)(Dearinger, Bryan) (Entered: 03/07/2014)
03/10/2014	96		Memorandum in opposition to re 85 MOTION For Entry Of Default And To Strike Government Defendants Answer To Plaintiffs Third Amended Complaint re 83 Answer to Amended Complaint, *(Government Defendants' Opposition to Plaintiffs' Motion to Strike Answer)* filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Text of Proposed Order)(Dearinger, Bryan) (Entered: 03/10/2014)
03/14/2014	97		REPLY to opposition to motion re 85 MOTION For Entry Of Default And To Strike Government Defendants Answer To Plaintiffs Third Amended Complaint re 83 Answer to Amended Complaint, filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Klayman, Larry) (Entered: 03/14/2014)
03/19/2014	98		LEAVE TO FILE DENIED− Motion for pro hac vice, electronic filing and modify judgment This document is unavailable as the Court denied its filing.. "Leave to file Denied" Signed by Judge Richard J. Leon on 03/19/2014. (jf,) (Entered: 03/20/2014)
03/20/2014	99		SUPPLEMENTAL MEMORANDUM to re 85 MOTION For Entry Of Default And To Strike Government Defendants Answer To Plaintiffs Third Amended Complaint re 83 Answer to Amended Complaint, filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Attachments: # 1 Exhibit 1 −− Return Receipt for the Honorable Roger VInson)(Klayman, Larry) (Entered: 03/20/2014)
03/24/2014	100		Memorandum in opposition to re 95 MOTION for Joinder *(Motion to Intervene)* filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Text of Proposed Order)(Dearinger, Bryan) (Entered: 03/24/2014)
03/24/2014	101		Memorandum in opposition to re 93 MOTION for Joinder MOTION to Intervene *Filed by David Andrew Christenson* filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Text of Proposed Order)(Dearinger, Bryan) (Entered: 03/24/2014)
03/26/2014	102		MOTION for Telephonic Status Conference by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Associated Press article about Jimmy Carter, # 2 Exhibit 2 −− Transcript of President Obama's Remarks from March 25, 2014, # 3 Text of Proposed Order)(Klayman, Larry) (Entered: 03/26/2014)
04/01/2014	103		MOTION to Compel *Defendants' Compliance With FRCP Rule 26* by LARRY E. KLAYMAN, MARY ANN STRANGE (Attachments: # 1 Text of Proposed Order)(Klayman, Larry) (Entered: 04/01/2014)
04/01/2014	104		Amended MOTION to Compel *Defendants' Compliance With FRCP Rule 26* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE

			(Attachments: # 1 Exhibit 1 −− Email from Obama Justice Department, # 2 Text of Proposed Order)(Klayman, Larry) (Entered: 04/01/2014)
04/07/2014			MINUTE ORDER denying 102 Plaintiffs' Motion for Telephonic Status Conference. It is hereby ORDERED that the motion is DENIED. Signed by Judge Richard J. Leon on 4/7/2014. (lcrjl1,) (Entered: 04/07/2014)
04/08/2014	105		LEAVE TO FILE DENIED− DAVID ANDREW CHRISTENSON, Motion for Emergency Stay This document is unavailable as the Court denied its filing. "Leave to file Denied". Signed by Judge Richard J. Leon. (Attachments: # 1 Exhibit) (zrdj) (Entered: 04/08/2014)
04/11/2014	106		MOTION To Remove Stay On Preliminary Injunction Order Of December 16, 2013 re 48 Memorandum & Opinion, 49 Order on Motion for Preliminary Injunction, by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Text of Proposed Order)(Klayman, Larry) (Entered: 04/11/2014)
04/11/2014	107		NOTICE *of Filing of Exhibit 1* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE re 106 MOTION To Remove Stay On Preliminary Injunction Order Of December 16, 2013 re 48 Memorandum & Opinion, 49 Order on Motion for Preliminary Injunction, (Klayman, Larry) (Entered: 04/11/2014)
04/15/2014	108		MOTION for Partial Summary Judgment by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Statement of Facts Not in Dispute, # 2 Text of Proposed Order)(Klayman, Larry) (Entered: 04/15/2014)
04/16/2014	109		REPLY to opposition to re (95 in 1:13−cv−00851−RJL, 69 in 1:13−cv−00881−RJL) MOTION for Joinder filed by TIMOTHY DEMITRI BROWN. "Leave to file Granted" signed by Judge Richard J. Leon (jf,) (Entered: 04/17/2014)
04/18/2014	110		Memorandum in opposition to re 103 MOTION to Compel *Defendants' Compliance With FRCP Rule 26* filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Exhibit CMO, # 2 Text of Proposed Order)(Patton, Rodney) (Entered: 04/18/2014)
04/24/2014	111		LEAVE TO FILE DENIED by David Andrew Christenson − Summary Judgment. This document is unavailable as the Court denied its filing.. "Leave to filed DENIED" Signed by Judge Richard J. Leon on 04/24/2014. (jf,) Modified on 4/24/2014 (jf,). (Entered: 04/24/2014)
04/28/2014			MINUTE ORDER denying as moot 52 Motion to Dismiss; denying as moot 52 Motion for Summary Judgment; denying as moot 55 Motion to Dismiss. In light of the parties' 75 Stipulation of Dismissal pursuant to Federal Rule of Civil Procedure 41(a)(1)(A)(ii), in which the parties jointly stipulated to the voluntary dismissal without prejudice of any and all claims by Plaintiffs against Defendants Verizon Communications Inc. and Lowell C. McAdam, it is hereby ORDERED that 55 Verizon Defendants' Motion to Dismiss is DENIED AS MOOT; and it is further ORDERED that 52 Government Defendants' Motion to Dismiss Claims Against the Verizon Defendants, or in the Alternative for Summary Judgment, is DENIED AS MOOT. Signed by

			Judge Richard J. Leon on 4/28/2014. (lcrjl1,) (Entered: 04/28/2014)
04/28/2014	112		NOTICE *Praecipe* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Motion To Strike and for Sanctions, # 2 Exhibit 2 −− Opposition to Motion to Strike and for Sanctions, # 3 Exhibit 3 −− Reply in Support of Motion to Strike and for Sanctions)(Klayman, Larry) (Entered: 04/28/2014)
04/28/2014	113		Memorandum in opposition to re 106 MOTION To Remove Stay On Preliminary Injunction Order Of December 16, 2013 re 48 Memorandum & Opinion, 49 Order on Motion for Preliminary Injunction, filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Text of Proposed Order)(Patton, Rodney) (Entered: 04/28/2014)
04/30/2014	114		REPLY to opposition to motion re 106 MOTION To Remove Stay On Preliminary Injunction Order Of December 16, 2013 re 48 Memorandum & Opinion, 49 Order on Motion for Preliminary Injunction, filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Klayman, Larry) (Entered: 04/30/2014)
05/01/2014	115		MOTION for Extension of Time to *Respond to Plaintiffs' Motion for Partial Summary Judgment* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 05/01/2014)
05/01/2014			MINUTE ORDER granting 115 Government Defendants' Motion for Extension of Time to Respond to Plaintiffs' Motion for Partial Summary Judgment. It is hereby ORDERED that the motion is GRANTED; and it is further ORDERED that Government Defendants shall have until 5/9/2014 to file their response to 108 Plaintiffs' Motion for Partial Summary Judgment. Signed by Judge Richard J. Leon on 5/1/2014. (lcrjl1,) (Entered: 05/01/2014)
05/01/2014			MINUTE ORDER denying 106 Plaintiffs' Motion to Remove Stay on Preliminary Injunction Order of December 16, 2013. It is hereby ORDERED that the motion is DENIED. Signed by Judge Richard J. Leon on 5/1/2014. (lcrjl1,) (Entered: 05/01/2014)
05/05/2014			Set/Reset Deadlines: Response to Motion for Partial Summary Judgment due by 5/9/2014. (tb,) (Entered: 05/05/2014)
05/08/2014	116		LEAVE TO FILE DENIED− Movant John Stritzinger's motion to reconsider admission, motion to compel and quash This document is unavailable as the Court denied its filing.. Signed by Judge Richard J. Leon on 5/8/14. (td,) (Entered: 05/09/2014)
05/09/2014	117		Memorandum in opposition to re 108 MOTION for Partial Summary Judgment *(Government Defendants' Opposition to Plaintiffs' Motion for Partial Summary Judgment)* filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Exhibit (Shea Declaration), # 2 Exhibit (March 20, 2014, FISC Order), # 3 Exhibit (Response to Plaintiffs' Statement of Material Facts), # 4 Text of Proposed Order)(Gilligan, James)

			(Entered: 05/09/2014)
05/19/2014	118		REPLY to opposition to motion re 108 MOTION for Partial Summary Judgment filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Klayman, Larry) (Entered: 05/19/2014)
05/21/2014	119		LEAVE TO FILE DENIED− Motion to Reconsider Admission, Motion to Compel, and Quash This document is unavailable as the Court denied its filing.. "Leave to file denied" Signed by Judge Richard J. Leon on 05/20/2014. (jf,) (Entered: 05/21/2014)
07/02/2014	120		NOTICE *of New Case Authority* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1 −− Riley v. California (case law))(Klayman, Larry) (Entered: 07/02/2014)
07/29/2014	121		LEAVE TO FILE DENIED− Non−party John Stritzinger's Motion for Pro Hace Vice, Motion for Electronic Filing, and Motion to Modify Judgment or Motion for Teleconference Hearing Prior to Appeal This document is unavailable as the Court denied its filing. (td,) (Entered: 07/29/2014)
07/30/2014			MINUTE ORDER. It is hereby ORDERED that Government Defendants' Motion for Extension of Time to Respond to Plaintiffs' Amended Complaints in Light of Memorandum Opinion Issued Today 51 is GRANTED nunc pro tunc. It is further ORDERED that Plaintiffs' Motion for Status Conference 63 is DENIED as moot. It is further ORDERED that Plaintiffs' Motion to Supplement the Record Concerning Recent Anonymous NSA Public Disclosures Over Metadata Collection 79 is DENIED. It is further ORDERED that Plaintiffs' Motion For Entry of Default and to Strike Government Defendants' Answer To Plaintiffs' Third Amended Complaint 85 is DENIED. It is further ORDERED that Motion to Join and/or Motion to Intervene by DAVID ANDREW CHRISTENSON 93 is DENIED. It is further ORDERED that MOTION to Join and for Leave by TIMOTHY DEMITRI BROWN 95 is DENIED. It is further ORDERED that Plaintiffs' Motion to Compel Defendants' Compliance With FRCP Rule 26 103 is DENIED. And it is further ORDERED that Plaintiffs' Amended Motion to Compel Defendants' Compliance With FRCP Rule 26 104 is DENIED. SO ORDERED. Signed by Judge Richard J. Leon on 7/30/2014. (lcrjl1,) (Entered: 07/30/2014)
07/30/2014			MINUTE ORDER granting 66 Government Defendants' Motion for Stay of Proceedings Against the Government Defendants Pending Appeal of Preliminary Injunction. It is hereby ORDERED that the motion is GRANTED; and it is further ORDERED that all proceedings against the Government Defendants in the above−captioned action are hereby STAYED pending the Government Defendants' appeal to the United States Court of Appeals for the District of Columbia Circuit from this Court's December 16, 2013, preliminary injunction in Case No. 13−cv−851. Signed by Judge Richard J. Leon on 7/30/2014. (lcrjl1,) (Entered: 07/30/2014)
08/08/2014	122		MOTION to Intervene by FREDERICK BANKS (jf,) (Entered: 08/11/2014)
08/22/2014	123		RESPONSE re 122 MOTION to Intervene *by Applicant Frederick Banks* filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Text of Proposed Order)(Patton, Rodney) (Entered: 08/22/2014)

08/22/2014	124		NOTICE OF APPEAL as to (in 1:13−cv−00851−RJL, 14 in 1:14−cv−00092−RJL, 78 in 1:13−cv−00881−RJL) Leave to File Denied, (105 in 1:13−cv−00851−RJL, 8 in 1:14−cv−00092−RJL, MINUTE ORDER in 1:13−cv−00881−RJL) Leave to File Denied by DAVID ANDREW CHRISTENSON. Fee Status: No Fee Paid. Parties have been notified. (jf,) Modified on 8/25/2014 (jf,). Modified on 8/25/2014 (jf,). (Entered: 08/25/2014)
08/25/2014	125		Transmission of the Notice of Appeal, Order Appealed, and Docket Sheet to US Court of Appeals. The Fee remains to be paid and another notice will be transmitted when the fee has been paid in the District Court re 124 Notice of Appeal,. (jf,) (Entered: 08/25/2014)
08/28/2014			USCA Case Number 14−5209 for 124 Notice of Appeal, filed by DAVID ANDREW CHRISTENSON. (kb) (Entered: 08/29/2014)
09/08/2014	126		MOTION for Leave to Appeal in forma pauperis by DAVID ANDREW CHRISTENSON (jf,) (Entered: 09/11/2014)
10/20/2014	127		ORDER of USCA (certified copy) as to (29 in 1:14−cv−00092−RJL) Notice of Appeal, filed by DAVID ANDREW CHRISTENSON ; USCA Case Number 14−5207. ORDERED, on the court's own motion, that these cases be held in abeyance pending the district court's resolution of appellant's motions for leave to proceed on appeal in forma pauperis. (kb) (Entered: 10/20/2014)
10/20/2014			MINUTE ORDER denying without prejudice 126 Motion for Leave to Appeal in forma pauperis. It is hereby ORDERED that the motion for leave to appeal in forma pauperis is DENIED without prejudice. Plaintiff is directed to file an affidavit accompanying the motion for permission to appeal in forma pauperis, for which there is a form available on the D.C. Circuit Court of Appeals' web site, in which Plaintiff must affirm the inability to prepay the docket fees for the appeal because of Plaintiff's poverty. Once such affidavit is filed, the Court shall reconsider the motion for leave to appeal in forma pauperis. Signed by Judge Richard J. Leon on 10/20/2014. (lcrjl1) (Entered: 10/20/2014)
10/21/2014	128		Supplemental Record on Appeal transmitted to US Court of Appeals re Order on Motion for Leave to Appeal in forma pauperis,, ;USCA Case Number 14−5207. (jf,) (Entered: 10/21/2014)
03/20/2015	129		MOTION for In Chambers and Ex Parte Interview of Witness Dennis Montgomery by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1, # 2 Exhibit 2, # 3 Exhibit 3, # 4 Exhibit 4, # 5 Text of Proposed Order)(Klayman, Larry) (Entered: 03/20/2015)
04/01/2015	130		MOTION to Lift Stay re 48 Memorandum & Opinion, 49 Order on Motion for Preliminary Injunction, by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Klayman, Larry) (Entered: 04/01/2015)
04/03/2015	131		MOTION for Extension of Time to File Response/Reply as to 129 MOTION for In Chambers and Ex Parte Interview of Witness Dennis Montgomery by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 04/03/2015)

04/06/2015			MINUTE ORDER granting 131 Motion for Extension of Time to File Response/Reply. It is hereby ORDERED that defendants' motion is GRANTED. It is further ORDERED that defendants shall have up to and including 4/13/2015 to file their opposition to plaintiff's motion for in chambers and ex parte interview of witness. Signed by Judge Richard J. Leon on 4/6/2015. (lcrjl1,) (Entered: 04/06/2015)
04/07/2015			Set/Reset Deadlines: Response due by 4/13/2015. (tb,) (Entered: 04/07/2015)
04/13/2015	132		RESPONSE re 129 MOTION for In Chambers and Ex Parte Interview of Witness Dennis Montgomery *(The Government Defendants Opposition To Plaintiffs Motion For In Chambers And Ex Parte Interview Of Witness Dennis Montgomery)* filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Text of Proposed Order, # 2 Exhibit 1, # 3 Exhibit 2, # 4 Exhibit 3, # 5 Exhibit 4, # 6 Exhibit 5, # 7 Exhibit 6, # 8 Exhibit 7, # 9 Exhibit 8, # 10 Exhibit 9, # 11 Exhibit 10, # 12 Exhibit 11)(Gilligan, James) (Entered: 04/13/2015)
04/20/2015	133		Memorandum in opposition to re 130 MOTION to Lift Stay re 48 Memorandum & Opinion, 49 Order on Motion for Preliminary Injunction, filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Text of Proposed Order)(Patton, Rodney) (Entered: 04/20/2015)
04/23/2015	134		REPLY to opposition to motion re 129 MOTION for In Chambers and Ex Parte Interview of Witness Dennis Montgomery filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Klayman, Larry) (Entered: 04/23/2015)
04/29/2015	135		REPLY to opposition to motion re 130 MOTION to Lift Stay re 48 Memorandum & Opinion, 49 Order on Motion for Preliminary Injunction, filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Klayman, Larry) (Entered: 04/29/2015)
05/12/2015	136		SUPPLEMENTAL MEMORANDUM to re 129 MOTION for In Chambers and Ex Parte Interview of Witness Dennis Montgomery , 130 MOTION to Lift Stay re 48 Memorandum & Opinion, 49 Order on Motion for Preliminary Injunction, *and Notice of New Case Authority* filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Attachments: # 1 Exhibit 1, # 2 Exhibit 2)(Klayman, Larry) (Entered: 05/12/2015)
05/27/2015	137		MANDATE of USCA (certified copy) as to (29 in 1:14−cv−00092−RJL, 124 in 1:13−cv−00851−RJL, 85 in 1:13−cv−00881−RJL) Notice of Appeal, filed by DAVID ANDREW CHRISTENSON. ORDERED that the motions be denied and, on the court's own motion, the appeal be dismissed as frivolous pursuant to 28 U.S.C. § 1915(e)(2)(B). USCA Case Numbers 14−5207, 14−5208 and 14−5209. (rd) (Entered: 05/28/2015)
05/29/2015	138		RESPONSE *to Plaintiffs' Supplement to Motion to Lift Stay Pending Appeal and Motion for In Camera Interview and Notice of New Case Authority* filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S.

			DEPARTMENT OF JUSTICE. (Berman, Julia) (Entered: 05/29/2015)
08/10/2015	139		ENTERED IN ERROR.....SUPPLEMENTAL MEMORANDUM to re 130 MOTION to Lift Stay re 48 Memorandum & Opinion, 49 Order on Motion for Preliminary Injunction, filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Klayman, Larry) Modified on 8/11/2015 (znmw). (Entered: 08/10/2015)
08/10/2015	140		SUPPLEMENTAL MEMORANDUM to re 130 MOTION to Lift Stay re 48 Memorandum & Opinion, 49 Order on Motion for Preliminary Injunction, *(Amended)* filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Attachments: # 1 Exhibit 1)(Klayman, Larry) (Entered: 08/10/2015)
08/11/2015			NOTICE OF CORRECTED DOCKET ENTRY: Docket Entry 139 Supplemental Memorandum was entered in error and refiled with an exhibit as Docket Entry 140 Supplemental Memorandum. (znmw) (Entered: 08/11/2015)
08/28/2015			Set/Reset Hearings: Status Conference set for 9/2/2015 12:00 PM in Courtroom 18 before Judge Richard J. Leon. (tb) (Entered: 08/28/2015)
08/31/2015	141		MOTION to Continue *the Status Conference Until the Following Week* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Patton, Rodney) (Entered: 08/31/2015)
08/31/2015			MINUTE ORDER denying 141 Motion to Continue. It is hereby ORDERED that government defendants' Motion to Continue the Status Conference set for 9/2/2015 at 12:00PM in Courtroom 18 before Judge Richard J. Leon is DENIED. Signed by Judge Richard J. Leon on 8/31/15. (lcrjl3,) (Entered: 08/31/2015)
08/31/2015	142		RESPONSE re 141 MOTION to Continue *the Status Conference Until the Following Week* filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Klayman, Larry) (Entered: 08/31/2015)
09/02/2015			Minute Entry for proceedings held before Judge Richard J. Leon: Status Conference held on 9/2/2015. (Court Reporter: William Zaremba) (jth) (Entered: 09/02/2015)
09/03/2015	143		TRANSCRIPT OF STATUS HEARING PROCEEDINGS before Judge Richard J. Leon held on September 2, 2015; Page Numbers: 1−48. Date of Issuance: September 3, 2015. Court Reporter/Transcriber: William Zaremba; Telephone number: (202) 354−3249; Court Reporter Email Address: WilliamPZaremba@gmail.com. For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi−page, condensed, PDF or ASCII) may be purchased from the court reporter. **NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty−one days to file with the court and the court reporter any request to

			redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov. Redaction Request due 9/24/2015. Redacted Transcript Deadline set for 10/4/2015. Release of Transcript Restriction set for 12/2/2015.(wz) (Entered: 09/03/2015)
09/03/2015	144		NOTICE *of Filing* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit A)(Klayman, Larry) (Entered: 09/03/2015)
09/08/2015	145		MOTION for Leave to File *Fourth Amended Complaint* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Text of Proposed Order)(Klayman, Larry) (Entered: 09/08/2015)
09/08/2015			MINUTE SCHEDULING ORDER: Given the exigencies presented by this case, it is hereby ORDERED that defendants' opposition to 145 Plaintiff's Motion for Leave to File Fourth Amended Complaint, if any, shall be filed no later than September 15, 2015. It is further ORDERED that the Court will hear oral argument regarding this motion on September 16, 2015 at 2:30PM. SO ORDERED. Signed by Judge Richard J. Leon on 9/8/15. (lcrjl3,) (Entered: 09/08/2015)
09/10/2015			Set/Reset Hearings: Motion Hearing set for 9/16/2015 02:30 PM in Courtroom 18 before Judge Richard J. Leon. (tb) (Entered: 09/10/2015)
09/15/2015	146		RESPONSE re 145 MOTION for Leave to File *Fourth Amended Complaint* filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK HUSSEIN OBAMA, II, U.S. DEPARTMENT OF JUSTICE. (Gilligan, James) (Entered: 09/15/2015)
09/16/2015			Minute Entry: Motion Hearing held on 9/16/2015 before Judge Richard J. Leon: re 145 MOTION for Leave to File *Fourth Amended Complaint* filed by LARRY E. KLAYMAN, MARY ANN STRANGE, CHARLES STRANGE; motion heard and GRANTED. Plaintiff's renewed motion for preliminary injunction due by 9/21/2015. Response due by COB on 10/1/2015. Reply due by COB on 10/5/2015. Motion Hearing set for 10/8/2015 02:00 PM in Courtroom 18 before Judge Richard J. Leon. (Court Reporter William Zaremba) (tb) (Entered: 09/16/2015)
09/17/2015	147		TRANSCRIPT OF MOTION HEARING PROCEEDINGS before Judge Richard J. Leon held on September 16, 2015; Page Numbers: 1−24. Date of Issuance: September 17, 2015. Court Reporter/Transcriber: William Zaremba; Telephone number: (202) 354−3249; Court Reporter Email Address: WilliamPZaremba@gmail.com. For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi−page, condensed, PDF or ASCII) may be purchased from the court reporter.

			NOTICE RE REDACTION OF TRANSCRIPTS: The parties have twenty−one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov. Redaction Request due 10/8/2015. Redacted Transcript Deadline set for 10/18/2015. Release of Transcript Restriction set for 12/16/2015.(wz) (Entered: 09/17/2015)
09/21/2015	148		LEAVE TO FILE DENIED− Motion to Intervene for Summary Judgment This document is unavailable as the Court denied its filing.. "Leave to file denied" Signed by Judge Richard J. Leon on 09/20/2015. (jf) (Entered: 09/21/2015)
09/21/2015	149		MOTION for Preliminary Injunction *(Renewed)* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1, # 2 Exhibit 2, # 3 Text of Proposed Order)(Klayman, Larry) (Entered: 09/21/2015)
10/01/2015	150		RESPONSE re 149 MOTION for Preliminary Injunction *(Renewed) (Government Defendants' Opposition to Plaintiffs' Renewed Motion for a Preliminary Injunction)* filed by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK OBAMA, U.S. DEPARTMENT OF JUSTICE. (Attachments: # 1 Exhibit 1, # 2 Exhibit 2, # 3 Exhibit 3, # 4 Exhibit 4, # 5 Exhibit 5, # 6 Exhibit 6, # 7 Text of Proposed Order 7)(Gilligan, James) (Entered: 10/01/2015)
10/02/2015	151		MOTION for Extension of Time to File Response/Reply as to 149 MOTION for Preliminary Injunction *(Renewed) (Nunc Pro Tunc)* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK OBAMA, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 10/02/2015)
10/05/2015	152		REPLY to opposition to motion re 149 MOTION for Preliminary Injunction *(Renewed)* filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE. (Attachments: # 1 Exhibit 1, # 2 Exhibit 2)(Klayman, Larry) (Entered: 10/05/2015)
10/06/2015			MINUTE ORDER granting government defendants' 151 Motion for a Three−Hour Extension of Time Nunc Pro Tunc to File the Government Defendants' Opposition to Plaintiff's Renewed Motion for a Preliminary Injunction. It is hereby ORDERED that government defendants' motion is GRANTED. Signed by Judge Richard J. Leon on 10/6/15. (lcrjl3,) (Entered: 10/06/2015)
10/06/2015	153		NOTICE *of Filing* by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE (Attachments: # 1 Exhibit 1)(Klayman, Larry) (Entered: 10/06/2015)
10/06/2015	154		MANDATE of USCA (certified copy) as to (46 in 1:13−cv−00881−RJL) Notice of Appeal to DC Circuit Court, filed by NATIONAL SECURITY AGENCY, KEITH B. ALEXANDER, BARACK OBAMA, ERIC H. HOLDER, JR., DEPARTMENT OF JUSTICE OF THE UNITED STATES, (67 in 1:13−cv−00851−RJL) Notice of Cross Appeal, filed by LARRY E.

			KLAYMAN, MARY ANN STRANGE, CHARLES STRANGE, (50 in 1:13−cv−00881−RJL) Notice of Cross Appeal, filed by MATT GARRISON, LARRY E. KLAYMAN, CHARLES STRANGE, MICHAEL FERRARI, (64 in 1:13−cv−00851−RJL) Notice of Appeal to DC Circuit Court, filed by NATIONAL SECURITY AGENCY, KEITH B. ALEXANDER, U.S. DEPARTMENT OF JUSTICE, BARACK OBAMA, ERIC H. HOLDER, JR. ORDERED and ADJUDGED that the preliminary injunction entered by the District Court be vacated and the cases are hereby remanded for such further proceedings as may be appropriate, in accordance with the opinion of the court filed herein this date. USCA Case Number 14−5004; Consolidated with 14−5005, 14−5016 and 14−5017. (rd) (Entered: 10/14/2015)
10/08/2015			MINUTE ORDER: It is hereby ordered that the time for the Motion Hearing today is CHANGED to 03:00 PM in Courtroom 18 before Judge Richard J. Leon. SO ORDERED − Judge Richard J. Leon on 10/08/15. (tb) (Entered: 10/08/2015)
10/08/2015			Minute Entry: Motion Hearing held on 10/8/2015 before Judge Richard J. Leon re 149 MOTION for Preliminary Injunction *(Renewed)* filed by LARRY E. KLAYMAN, MARY ANN STRANGE, CHARLES STRANGE; Motion heard and taken under advisement. (Court Reporter William Zaremba) (tb) (Entered: 10/09/2015)
10/19/2015	155		TRANSCRIPT OF MOTION HEARING PROCEEDINGS before Judge Richard J. Leon held on October 8, 2015; Page Numbers: 1−45. Date of Issuance: October 19, 2015. Court Reporter/Transcriber: William Zaremba; Telephone number: (202) 354−3249; Transcripts may be ordered by submitting the Transcript Order Form. For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi−page, condensed, PDF or ASCII) may be purchased from the court reporter. **NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty−one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov. Redaction Request due 11/9/2015. Redacted Transcript Deadline set for 11/19/2015. Release of Transcript Restriction set for 1/17/2016.(wz) (Entered: 10/19/2015)
10/29/2015	156		NOTICE OF SUPPLEMENTAL AUTHORITY by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK OBAMA, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Exhibit)(Patton, Rodney) (Entered: 10/29/2015)
10/29/2015	157		RESPONSE re 156 NOTICE OF SUPPLEMENTAL AUTHORITY filed by LARRY E. KLAYMAN, CHARLES STRANGE, MARY ANN STRANGE.

			(Klayman, Larry) (Entered: 10/29/2015)
11/09/2015	158	33	MEMORANDUM OPINION. Signed by Judge Richard J. Leon on 11/09/15. (tb) Modified on 11/9/2015 (tb). (Entered: 11/09/2015)
11/09/2015	159	76	ORDER: For the reasons set forth in the Memorandum Opinion entered this date; it is hereby ordered that plaintiffs' 149 Renewed Motion for Preliminary Injunction is GRANTED as to plaintiff J.J. Little and J.J Little & Associates, P.C. and DENIED as to plaintiffs Larry Klayman, Charles Strange and Mary Ann Strange; it is further ordered that the government: (1) is barred from collecting, as part of the NSA's Bulk Telephony Metadata Program, any telephone metadata associated with J.J. Little and J.J. Little & Associates, P.C. Verizon Business Network Services telephone subscriptions; and (2) must segregate out all such metadata already collected from any future searches of its metadata database. Signed by Judge Richard J. Leon on 11/09/15. (tb) Modified on 11/9/2015 (tb). (Entered: 11/09/2015)
11/09/2015	160		Emergency MOTION to Stay *the Court's Preliminary Injunction Pending Appeal and for an Immediate Administrative Stay* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK OBAMA, U.S. DEPARTMENT OF JUSTICE (Attachments: # 1 Proposed Order 1, # 2 Proposed Order 2)(Gilligan, James) (Entered: 11/09/2015)
11/10/2015			MINUTE ORDER: For the reasons discussed at length in my Memorandum Opinion issued November 9, 2015, Klayman v. Obama, Civ. No. 13−851−(RJL) [Dkt. #158], it is hereby ORDERED that the Government Defendants' Emergency Motion for a Stay of the Court's Preliminary Injunction Pending Appeal and for an Immediate Administrative Stay [Dkt. #160] is DENIED. SO ORDERED. Signed by Judge Richard J. Leon on 11/10/2015. (lcrjl3,) (Entered: 11/10/2015)
11/10/2015	161		ENTERED IN ERROR.....NOTICE *of Appeal* by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK OBAMA, U.S. DEPARTMENT OF JUSTICE (Patton, Rodney) Modified on 11/10/2015 (jf). (Entered: 11/10/2015)
11/10/2015	162	31	NOTICE OF INTERLOCUTORY APPEAL as to 158 Memorandum & Opinion, 159 Order on Motion for Preliminary Injunction,,, by KEITH B. ALEXANDER, ERIC H. HOLDER, JR, NATIONAL SECURITY AGENCY, BARACK OBAMA, U.S. DEPARTMENT OF JUSTICE. Fee Status: No Fee Paid. Parties have been notified. (Patton, Rodney) (Entered: 11/10/2015)

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. 1:13-cv-00851-RJL

GOVERNMENT DEFENDANTS' NOTICE OF APPEAL

Defendants Barack Obama, President of the United States, Loretta E. Lynch, Attorney General of the United States, and Admiral Michael S. Rogers, Director of the National Security Agency ("NSA"), insofar as they are sued in their official capacities, together with defendants NSA and the United States Department of Justice (collectively, the "Government Defendants"), hereby appeal to the United States Court of Appeals for the District of Columbia Circuit from the November 9, 2015 Order (ECF No. 159) and Memorandum Opinion (ECF No. 158) granting Plaintiffs' Renewed Motion for Preliminary Injunction (ECF No. 149) as to Plaintiffs J.J. Little and J.J. Little & Associates, P.C.

Dated: November 10, 2015

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ Rodney Patton
JAMES J. GILLIGAN
Special Litigation Counsel
RODNEY PATTON
JULIA A. BERMAN
CAROLINE J. ANDERSON
Trial Attorneys

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7320
Washington, D.C. 20044
Phone: (202) 305-7919
Fax: (202) 616-8470
E-mail: rodney.patton@usdoj.gov

Counsel for the Government Defendants

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KLAYMAN et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	**Civil Action No. 13-851 (RJL)**
	)	
OBAMA et al.,	)	
	)	
Defendants.	)	

MEMORANDUM OPINION
November 9, 2015 [Dkt. #149]

Our Circuit Court has remanded this case for me to determine whether limited discovery is appropriate to satisfy the standing requirements set forth by the Supreme Court in an earlier national security surveillance case: *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013). Although familiarity with the record and my prior opinion on December 16, 2013[1] is likely, I will briefly recount the history of this matter.

On November 18, 2013, I held a hearing on a motion filed by plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange to preliminarily enjoin the National Security Agency ("NSA") from collecting and querying their telephony metadata pursuant to the NSA's classified bulk telephony metadata collection program (the "Bulk Telephony Metadata Program" or the "Program"), under which the NSA indiscriminately

[1] *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

collects the telephone call records of millions of Americans. Four weeks later, on December 16, 2013, I issued a lengthy opinion ("my December 2013 Opinion") granting the motion as to plaintiffs Larry Klayman and Charles Strange after finding that they had demonstrated a substantial likelihood of success on their Fourth Amendment claim that the collection and querying of their records constituted an unconstitutional search. However, because of the novelty of the legal issues presented and the monumental national security interests at stake, I stayed the injunction pending the appellate review that would undoubtedly follow. Indeed, I assumed that the appeal would proceed expeditiously, especially considering that the USA PATRIOT Act, the statute pursuant to which the NSA was acting, was due to expire on June 1, 2015—a mere eighteen months later. For reasons unknown to me, it did not. Instead, our Circuit Court heard argument on November 4, 2014 and did not issue its decision until August 28, 2015—nearly three months *after* the USA PATRIOT Act had lapsed and had been replaced by the USA FREEDOM Act, which was enacted on June 2, 2015.

As it pertains to this Opinion, the USA FREEDOM Act specifically prohibits the bulk collection of telephony metadata, but not until November 29, 2015. During the intervening 180-day period, the NSA is continuing to operate the Bulk Telephony Metadata Program while it transitions to a new, more targeted program whereby the NSA, pursuant to authorization by the Foreign Intelligence Surveillance Court ("FISC"), can require telecommunications service providers to run targeted queries against their customers' telephony metadata records and then produce the results of those queries to the NSA. Thus, when our Circuit Court issued its decision on August 28, 2015 vacating

my preliminary injunction for a lack of standing and remanding the case to this Court for further proceedings consistent therewith, nearly half of the 180-day transition period had already lapsed.

As a consequence, I immediately scheduled a status conference for the following week to discuss with the parties how to proceed, if at all, prior to the mandate issuing from the Court of Appeals.[2] On August 31, 2015, the Government moved to continue the status conference. I denied that motion. At the status conference on September 2, 2015, Mr. Klayman indicated, among other things, that he intended to seek expedited issuance of the mandate from the Court of Appeals and to amend his complaint by joining new parties who are customers of Verizon Business Network Services ("VBNS") and who therefore, consistent with the Court of Appeals decision, likely had standing to challenge the Program. As expected, on September 8, 2015, plaintiffs sought leave to file a Fourth Amended Complaint that adds plaintiffs J.J. Little and his law firm, J.J. Little & Associates, P.C. ("Little plaintiffs"), both of which are, and at "all material times" were,

---

[2] Once a case is appealed, a district court lacks jurisdiction over "those aspects of the case involved in the appeal" until the court of appeals issues its mandate. *Griggs v. Provident Consumer Discount Co.*, 459 U.S. 56, 58 (1982) ("The filing of a notice of appeal is an event of jurisdictional significance—it confers jurisdiction on the court of appeals and divests the district court of its control over those aspects of the case involved in the appeal"); *see also United States v. Defries*, 129 F.3d 1293, 1302 (D.C. Cir. 1997) ("The district court does not regain jurisdiction over those issues [that have been appealed] until the court of appeals issues its mandate."). Under the Federal Rules of Appellate Procedure, the mandate will not issue until "7 days after the time to file a petition for rehearing expires, or 7 days after entry of an order denying a timely petition for panel rehearing, petition for rehearing en banc, or motion for stay of mandate, whichever is later." Fed. R. App. P. 41(b). However, the Court of Appeals has "discretion to direct immediate issuance of its mandate in an appropriate case" and parties have "the right . . . at any time to move for expedited issuance of the mandate for good cause shown." D.C. Cir. R. 41(a)(1).

VBNS subscribers. Fourth Am. Compl. ¶ 18 [Dkt. #145-1]. At a September 16, 2015 hearing on this motion, I granted plaintiffs' motion to amend the complaint—which was uncontested—and set a briefing schedule for a renewed motion for preliminary injunction. On September 21, 2015, plaintiffs filed a Renewed Motion for Preliminary Injunction [Dkt. #149], seeking to enjoin as unconstitutional the Bulk Telephony Metadata Program, which is still in operation until November 29, 2015. On October 6, 2015, the Court of Appeals issued its mandate. I heard oral argument on plaintiffs' renewed motion for preliminary injunction two days later.

After careful consideration of the parties' pleadings, the representations made at the October 8, 2015 motion hearing, and the applicable law, I have concluded that limited discovery is not necessary since several of the plaintiffs now are likely to have standing to challenge the constitutionality of the Bulk Metadata Collection Program, and those that do have standing are entitled to preliminary injunctive relief. Accordingly, the Court will GRANT, in part, plaintiffs' Renewed Motion for Preliminary Injunction as it pertains to plaintiffs J.J. Little and J.J. Little & Associates and ENJOIN the future collection and querying of their telephone record metadata.

BACKGROUND

A brief overview of the statutory framework and procedural posture, focusing on developments since my last Opinion in this case, may be a helpful place to start.

A. Statutory Framework

1. The Section 215 Bulk Telephony Metadata Program

Beginning in 1998, the Foreign Intelligence Surveillance Act ("FISA") permitted the FBI to merely apply for an ex parte order authorizing specified entities, such as common carriers, to release to the FBI copies of "business records" upon 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." Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, § 602, 112 Stat. 2396, 2410 (1998). Following the September 11, 2001 terrorist attacks, however, Congress expanded this "business records" provision under Section 215 of the USA PATRIOT Act, to authorize the FBI to apply "for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 501, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861(a)(1)). Thereafter, in March 2006, Congress strengthened the protections in Section 215, amending the statute to provide that the FBI's application must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." USA PATRIOT

Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192, 196 (2006) (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

Although the daily bulk collection, storage, and analysis of telephony metadata is not expressly authorized by the terms of Section 215, beginning in May 2006, the Government, advocating a very aggressive reading of Section 215, sought and received FISC authorization to operate the Bulk Telephony Metadata Program, which, of course, consists of these very practices. *See* Decl. of Acting Assistant Dir. Robert J. Holley, FBI ¶ 6 [Dkt. #25-5] ("Holley Decl."); Decl. of Teresa H. Shea, Signals Intelligence Dir., NSA ¶ 13 [Dkt. # 25-4] ("Shea Decl."); *see also* Decl. of Major General Gregg C. Potter, Signals Intelligence Deputy Dir., NSA ¶ 2 [Dkt. #150-4] ("Potter Decl."). The FISC has repeatedly endorsed this view ever since. Shea Decl. ¶¶ 13-14.[3] As such, for more than seven years, the Government has obtained ex parte orders from the FISC directing telecommunications service providers to produce, on a daily basis, the telephony metadata for each of their subscriber's calls—this includes the dialing and receiving numbers and the date, time, and duration of the calls. It does not, however, include the substantive content of the call. Shea Decl. ¶¶ 7, 13-15, 18; *see* Primary Order, *In re Application of the [FBI] for an Order Requiring the Prod. of Tangible Things From [Redacted]*, No. BR 13-158 at 3 n.1 (FISC Oct. 11, 2013) (attached as Ex. B to Gilligan

[3] Notably, the Second Circuit recently disagreed, holding that, although Section 215 of the USA PATRIOT Act "sweeps broadly," it did not authorize the indiscriminate, daily bulk collection of metadata. *ACLU v. Clapper*, 785 F.3d 787, 821 (2d Cir. 2015) ("For all of the above reasons, we hold that the text of § 215 cannot bear the weight the government asks us to assign to it, and that it does not authorize the telephone metadata program. We do so comfortably in the full understanding that if Congress chooses to authorize such a far-reaching and unprecedented program, it has every opportunity to do so, and to do so unambiguously.").

Decl.) [Dkt. #25-3] ("Oct. 11, 2013 Primary Order"). Once this data is collected from various telecommunications companies, it is consolidated and retained in a single Government database for five years. *See* Shea Decl. ¶¶ 23, 30; *see* Oct. 11, 2013 Primary Order at 14 ¶ E. In this database, the NSA conducts computerized searches that are designed to discern whether certain terrorist organizations are communicating with persons located in the United States. Holley Decl. ¶ 5; Shea Decl. ¶¶ 8-10, 44-63; *see* Am. Mem. Op., *In re Application of the [FBI] for an Order Requiring the Prod. of Tangible Things from [REDACTED]*, No. BR 13-109 at 18-22 (FISC Aug. 29, 2013) (attached as Ex. A to Gilligan Decl.) [Dkt. #25-2]. Despite the Program's broad reach, since a series of leaks exposed the existence of this Program in 2013, the Government has maintained that it "has never captured information on all (or virtually all) calls made and/or received in the U.S." Gov't's Opp'n 5.

Shortly after my December 2013 Opinion, however, President Obama issued an order requiring several important changes to the manner in which these searches are authorized and conducted. *See* President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence; Potter Decl. ¶¶ 5-7. As initially authorized by the FISC, NSA intelligence analysts could conduct searches in the database *without* prior judicial authorization.[4] *See* Shea Decl. ¶ 19. This is no longer

[4] Searches in the database are conducted using "identifiers" such as suspected terrorist telephone numbers—so-called "seeds"— to "chain" or elucidate terrorist communications within the United States. Prior to January 2014, an "identifier" had to be approved by one of twenty-two designated officials in the NSA's Homeland Security Analysis Center or other parts of the

the case. Rather, except in emergency circumstances, NSA analysts are now required to seek approval from the FISC prior to conducting database queries. Potter Decl. ¶ 7. The FISC may only authorize a search if there is a "reasonable, articulable suspicion" ("RAS") that the selection term to be queried (i.e., the "identifier" or "seed") is associated with one or more of the specified foreign terrorist organizations approved for targeting by the FISC. *Id.* Moreover, at the time of my previous Opinion, query results included communication records within "three hops" of the seed identifier. *See* Shea Decl. ¶ 22. Since President Obama's order in January 2014, however, query results have been limited to records of communications within *two* "hops" from the seed, not three. Pottter Decl. ¶ 7. Stated differently, the query results include identifiers and the associated metadata having direct contact with the seed (the first "hop") and identifiers and associated metadata having a direct contact with first "hop" identifiers (the second "hop"). It remains the case that once a query is conducted and it returns a universe of responsive records, NSA analysts may then perform new searches and otherwise perform intelligence analysis *within* that universe of data without using RAS-approved search terms. *See* Shea Decl. ¶ 26.

2. The USA FREEDOM Act

Reacting to significant public outcry regarding the existence of the Bulk Telephony Metadata Program, President Obama called upon Congress to replace the

---

NSA's Signals Intelligence Directorate. Shea Decl. ¶¶ 19, 31. Such approval could be given only upon a determination by one of those designated officials that there exist facts giving rise to a "reasonable, articulable suspicion" ("RAS") that the selection term to be queried is associated with one or more of the specified foreign terrorist organizations approved for targeting by the FISC. *Id.* ¶¶ 20, 31; Holley Decl. ¶¶ 15-16.

Program with one that would "give the public greater confidence that their privacy is appropriately protected," while maintaining the intelligence tools needed "to keep us safe." President Barack Obama, Statement by the President on the Section 215 Bulk Metadata Program (Mar. 27, 2014), http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program. In response to this directive, Congress ultimately enacted the USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015) ("USA FREEDOM Act"), on June 2, 2015. Relevant to this Opinion, the USA FREEDOM Act expressly prohibits the Government from obtaining telephony metadata in bulk, but not until November 29, 2015. USA FREEDOM Act §§ 103, 109; *see* Potter Decl. ¶ 11. It seems that the NSA requested this 180-day delay to allow time to transition from the Bulk Telephony Metadata Program to a new replacement program Congress conceived—a model whereby targeted queries will be carried out against metadata held by telecommunications service providers and the resulting data subsequently produced to the Government. *See id.* § 101. As the Government has explained, this 180-day transition period will avoid a so-called "intelligence gap" that would follow if the current Program terminated before the new targeted metadata querying program is fully operational. Gov't's Opp'n 34; *see* 161 Cong. Rec. S3275 (daily ed. May 22, 2015) (statement of Sen. Leahy) (having printed in the record a letter from the NSA which stated: "NSA assesses that the transition of the program to a query at the provider model is achievable within 180 days, with provider cooperation. . . . [W]e 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."). To date, however, the Government has failed to identify any concrete consequences that would likely result from this so-called "intelligence gap." And while Congress refrained for obvious political reasons from expressly authorizing a six-month extension of the Bulk Telephony Metadata Program,[5] the Government conveniently went immediately thereafter to the FISC to seek judicial authorization to continue the Program during the transition period, consistent with its prior authorization under the USA PATRIOT Act. *See* Mem. of Law 5, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, No. BR 15-75 (FISC June 2, 2015). Not surprisingly, the FISC agreed. *See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, No. BR 15-75 (FISC June 29, 2015). As such, during the current 180-day transition period, the Bulk Telephony Metadata Program has continued by judicial, not legislative, fiat.[6]

B. Procedural Posture

I first had occasion to address plaintiffs' constitutional challenges to the Program in December 2013, when I enjoined the Government from further collecting plaintiffs'

[5] The enactment of the USA FREEDOM Act has been described as "signal[ing] a cultural turning point for the nation, almost 14 years after the Sept. 11 attacks heralded the construction of a powerful national security apparatus," which began with significant public backlash to the June 2013 revelation that the NSA was operating a classified bulk metadata collection program. Jennifer Steinhauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 is Sharply Limited*, N.Y. Times, Jun. 3, 2015, at A1.

[6] It is possible that the metadata collected and stored prior to November 29, 2015 will be retained for some period of time after that date to (1) meet any applicable preservation obligations in pending litigation and (2) conduct technical analysis for a three-month period to ensure that the production of call-detail records under the targeted collection program yields similar results to queries of metadata under the retiring Program. Potter Decl. ¶ 15. In any event, the Government represents that analytic access to the data will cease on November 29, 2015. *Id.*

call records under the Program. *Klayman v. Obama*, 957 F. Supp. 2d 1, 44-45 (D.D.C. 2013) (Leon, J.). I concluded, in so ruling, that plaintiffs Klayman and Charles Strange likely had standing to challenge both the bulk collection of metadata under the Program and the ensuing analysis of that data through the NSA's electronic querying process.[7] *Id.* at 26-29. As to the merits of plaintiffs' claims, I found it significantly likely that plaintiffs would be able to prove that the Program violated their reasonable expectation of privacy and therefore was a Fourth Amendment search. *Id.* at 30-37. I held, moreover, that the Program likely failed to meet the Fourth Amendment's reasonableness requirement because the substantial intrusion occasioned by the Program far outweighed any contribution to national security. *Id.* at 37-42. Because the loss of constitutional freedoms is an "irreparable injury" of the highest order, and relief to two of the named plaintiffs would not undermine national security interests, I found that a preliminary injunction was not merely warranted—it was *required*. *Id.* at 42-43. Cognizant, however, of the "significant national security interests at stake," and optimistic that our Circuit Court would expeditiously address plaintiffs' claims, I voluntarily stayed my order pending appeal. *See id.* at 43-44.

As stated previously, our Circuit Court did not do so. Moreover, when it finally issued its decision on August 28, 2015, it did so with considerable brevity. In three separate opinions, the Circuit Court vacated my preliminary injunction on the ground that

[7] Because plaintiffs pled no facts showing that plaintiff Mary Ann Strange was a Verizon Wireless subscriber, let alone a subscriber of any other phone services, I found that she lacked standing to pursue her claims and therefore restricted the remainder of my analysis to the claims advanced by plaintiffs Larry Klayman and Charles Strange. *See Klayman*, 957 F Supp. 2d at 8 & n.5, 43 n.69.

plaintiffs, as subscribers of Verizon Wireless rather than as subscribers of VBNS—the sole provider the Government has acknowledged has participated in the Program—had not shown a substantial likelihood of standing to pursue their claims. *Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015) (per curiam).[8] Left undecided—indeed wholly untouched—was the question of whether a program that indiscriminately collects citizens' telephone metadata constitutes an unconstitutional search under the Fourth Amendment.

Not surprisingly, plaintiffs moved for, and quickly obtained, leave to file a Fourth Amended Complaint. *See* Sept. 16, 2015 Min. Entry. This latest iteration of the Complaint alters plaintiffs' contentions in two material respects. First, it adds plaintiffs J.J. Little and his law firm, J.J. Little & Associates, P.C., both of which are, and at "all material times" were, VBNS subscribers. Fourth Am. Compl. ¶ 18.[9] Second, it sets forth

---

[8] Judge Brown concluded that plaintiffs had demonstrated a *possibility* that their call records are, or were, collected, but because they had not shown a *substantial likelihood* that this was the case, they fell "short of meeting the higher burden of proof required for a preliminary injunction." *Id.* at 562-64. Judge Williams opined that because "[p]laintiffs are subscribers of Verizon Wireless, not of Verizon Business Network Services, Inc.—the sole provider that the government has acknowledged targeting for bulk collection," plaintiffs "lack direct evidence that records involving their calls have actually been collected." *Id.* at 565 (Williams, J.). Given that the Government has neither confirmed nor denied Verizon Wireless's participation in the Program, Judge Williams found plaintiffs' inference that their data was collected too speculative to "demonstrate a 'substantial likelihood' of injury." *Id.* at 566. Judge Sentelle "agree[d] with virtually everything in Judge Williams' opinion," save for his conclusion that the case should be remanded instead of dismissed. *Id.* at 569-70. Like Judge Williams, Judge Sentelle opined that plaintiffs "never in any fashion demonstrate[d] that the [G]overnment is or has been collecting [call-detail] records from their [carrier]" and that the Supreme Court's rejection of similar inferential leaps in *Clapper v. Amnesty International, USA*, 133 S. Ct. 1138 (2013), counsels against finding standing here. *Id.* at 569.

[9] Plaintiffs furnished additional support for this claim in the Supplemental Declaration of J.J. Little, in which he avers that "I and my law firm J.J. Little Associates, P.C. have been customers (subscribers) of Verizon Business Network Services and also Verizon Wireless since October

additional facts intended to bolster plaintiffs' allegation that Verizon Wireless participated in the Program. *Id.* ¶¶ 47-48.

On September 21, 2015, plaintiffs filed a renewed motion for a preliminary injunction, seeking relief, once again, from the "warrantless surveillance" of their telephone calls. *See* Plaintiffs' Renewed Mot. for Prelim. Inj. & Req. for Oral Arg. Thereon [Dkt. #149]. Government defendants, of course, opposed, *see* Government Defendants' Opposition to Plaintiffs' Renewed Motion for a Preliminary Injunction [Dkt. #150] ("Gov't's Opp'n"), and plaintiffs quickly lodged their reply, *see* Plaintiffs' Reply in Support of their Renewed Motion for Preliminary Injunction [Dkt. #152]. On October 6, 2015, our Circuit Court granted plaintiffs' unopposed request for expedited issuance of the mandate, Order, *Obama v. Klayman*, No. 14-5004 (D.C. Cir. Oct. 6, 2015), thereby reinstating this Court's jurisdiction to decide plaintiffs' renewed motion, *see* Mandate [Dkt. #154]. I took plaintiffs' motion under advisement at the conclusion of oral argument on October 8, 2015.

ANALYSIS

I will confine my analysis to the merits of plaintiffs' request for a preliminary injunction and will not address the jurisdictional predicate for my actions, which I discussed at length in my December 2013 Opinion.[10] When ruling on a motion for

---

2011, and have been so continuously during the period from October 2011 until the present." Suppl. Decl. of J.J. Little [Dkt. #152-1].

[10] Specifically, I discussed this Court's jurisdictional authority to review plaintiffs' constitutional claims. *See Klayman*, 957 F. Supp. 2d at 24-25. In sum, I found that Congress had not stated with the requisite clarity any intent to preclude judicial review of constitutional claims related to FISC orders by any non-FISC courts. *See Webster v. Doe*, 486 U.S. 592, 603 (1988) ("[W]here

preliminary injunction, a court must consider "whether (1) the plaintiff has a substantial likelihood of success on the merits; (2) the plaintiff would suffer irreparable injury were an injunction not granted; (3) an injunction would substantially injure other interested parties; and (4) the grant of an injunction would further the public interest." *Sottera, Inc. v. Food & Drug Admin.*, 627 F.3d 891, 893 (D.C. Cir. 2010) (internal quotation marks omitted).[11] I will address each of these factors in turn.

A. Plaintiffs Have Shown a Substantial Likelihood of Success on the Merits.

My analysis of plaintiffs' likelihood of success on the merits of their constitutional claims focuses exclusively on their Fourth Amendment challenges, which I find most likely to succeed.[12] I begin, however, as I did previously, with plaintiffs' standing to

---

Congress intends to preclude judicial review of constitutional claims its intent to do so must be clear."); *see also Elgin v. Dep't of the Treasury*, 132 S. Ct. 2126, 2132 (2012) ("[A] necessary predicate to the application of *Webster*'s heightened standard [is] a statute that purports to deny any judicial forum for a colorable constitutional claim." (internal quotation marks omitted)); *McBryde v. Comm. to Review Circuit Council Conduct & Disability Orders of the Judicial Conference of the U.S.*, 264 F.3d 52, 59 (D.C. Cir. 2001) (finding "preclusion of review for both as applied and facial constitutional challenges only if the evidence of congressional intent to preclude is 'clear and convincing'").

[11] Our Circuit has traditionally applied a "sliding scale" approach to these four factors. *Davis v. Pension Benefit Guar. Corp.*, 571 F.3d 1288, 1291-92 (D.C. Cir. 2009). In other words, "a strong showing on one factor could make up for a weaker showing on another." *Sherley v. Sebelius*, 644 F.3d 388, 392 (D.C. Cir. 2011). Following the Supreme Court's decision in *Winter v. NRDC, Inc.*, 555 U.S. 7 (2008), however, our Circuit suggested, without deciding, that "*Winter* could be read to create a more demanding burden." *Davis*, 571 F.3d at 1292. Thus, while it is unclear whether the "sliding scale" remains controlling in light of *Winter*, the Court need not decide that issue today because I conclude that plaintiffs have carried their burden of persuasion as to all four factors.

[12] The Second Circuit recently declined to issue a preliminary injunction in a similar case, holding that the USA FREEDOM Act authorized the 180-day continuation of the Bulk Telephony Metadata Program and declining to reach the "momentous constitutional issues" raised by the limited continuation of the Program. *ACLU v. Clapper*, No. 14-42-cv (2d Cir. Oct. 29, 2015). In refusing to consider the constitutional questions raised, the Second Circuit noted that it "ought not meddle with Congress's considered decision" to continue the Program for a

challenge the Bulk Telephony Metadata Program. *See Jack's Canoes & Kayaks, LLC v. Nat'l Park Serv.*, 933 F. Supp. 2d 58, 76 (D.D.C. 2013) ("The first component of the likelihood of success on the merits prong usually examines whether the plaintiffs have standing in a given case." (internal quotation marks omitted)).

1. Plaintiffs are Substantially Likely to Have Standing to Challenge the Bulk Telephony Metadata Program.

Plaintiffs Larry Klayman, Charles Strange, Mary Ann Strange, J.J. Little, and J.J. Little & Associates, P.C. challenge the past and future collection of their telephone metadata, as well as the analysis of that data through the NSA's electronic querying process. After careful consideration of these challenges, I conclude that while plaintiffs J.J. Little and J.J. Little & Associates, P.C. have standing to proceed, plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange do not.

No principle is more fundamental to the balance of federal power 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 omitted). Inherent in this principle is the requirement that each plaintiff demonstrate adequate standing to press their claims in federal court. *Raines v. Byrd*, 521 U.S. 811, 818 (1997). "To establish Article III standing, an injury must be 'concrete,

---

limited transition period and that doing so would not be a "prudent use of judicial authority" given that rendering a decision on such difficult constitutional questions would almost certainly take longer than the time remaining for the Program's operation. *Id.* at 23. Fortunately for this Court, my analysis of these "momentous constitutional issues" began nearly two years ago, and so I do not suffer the same time constraints. Moreover, as I explain below, this Court cannot, and will not, sit idle in the face of likely constitutional violations for fear that it might be viewed as meddling with the decision of a legislative branch that lacked the political will, or votes, to *expressly* and unambiguously authorize the Program for another six months.

particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Clapper v. Amnesty Int'l USA* ("*Clapper*"), 133 S. Ct. 1138, 1147 (2013) (quoting *Monsanto Co. v. Geerston Seed Farms*, 561 U.S. 139, 149 (2010)); *see also Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 & n.1 (1992) ("By particularized, we mean that the injury must affect the plaintiff in a personal and individual way."). When the challenged harm is prospective, courts face the additional hurdle of assuring themselves that its likelihood is not too far flung, lest imminence, "a somewhat elastic concept . . . be stretched beyond its purpose" to create a controversy where none exists. *Lujan*, 504 U.S. at 564 n.2. Consequently, the "threatened injury must be *certainly impending*" to prevent litigation of illusory claims. *See Clapper*, 133 S. Ct. at 1147 (internal quotation marks omitted).

Any discussion of standing to challenge a classified Government surveillance program must begin with the seminal case on this issue: *Clapper v. Amnesty International*. *Clapper* concerned a challenge by Amnesty International to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881a, which authorizes the Government to surveil non-United States persons reasonably believed to be located outside the United States. 133 S. Ct. at 1142. There, plaintiffs, "United States persons whose work . . . requires them to engage in sensitive international communications with individuals who they believe are likely targets of surveillance under § 1881a," sought declaratory and injunctive relief from surveillance under the statute. *Id.* The issue before the Supreme Court was whether plaintiffs had standing to seek prospective relief. They did not. According to the Supreme Court, plaintiffs' claims

failed because their allegations rested on a series of contingencies that may—or may not—come to pass. Specifically, success required: that plaintiffs' foreign contacts would be targeted for surveillance under the challenged statute; that the FISC would approve the surveillance; that the government would *actually* intercept communications from plaintiffs' foreign contacts; and that plaintiffs' communications would be among those captured. *Id.* at 1148. Without reaching the merits of plaintiffs' claims, the Supreme Court held that plaintiffs had not established standing because their "theory of *future* injury [was] too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'" *Id.* at 1143 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). Whether *Clapper's* use of the term "certainly impending" imposes a higher threshold for standing, or merely adds gloss to the longstanding requirement of "concreteness," is unclear.[13] What *Clapper* does instruct, however, is that standing to challenge a classified Government surveillance program demands more than speculation that the challenged surveillance has, or will, transpire.

[13] As the *Clapper* majority pointed out in a footnote, "[o]ur cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur." *Clapper*, 133 S. Ct. at 1150 n.5. The Court declined, however, to comment further because it found plaintiffs' allegations too "attenuated" to demonstrate harm. Indeed, Justice Breyer, in his dissent, expressed doubt as to whether there is a meaningful difference between a "substantial risk" of future harm and a risk of "clearly impending harm." *Id.* at 1160-61 (Breyer, J., dissenting). In his view, "the case law uses the word 'certainly' as if it emphasizes, rather than literally defines, the immediately following term 'impending.'" *Id.* at 1161 (Breyer, J., dissenting). That is to say, whether "substantial risk" and "clearly impending" impose substantively different standing requirements, or lexical variations of the same overarching standard, is a question for another day. In any event, I need not reach this issue because I find that the Little plaintiffs have met the threshold for "certainly impending" injury.

On appeal here, our Circuit Court found that plaintiffs Klayman and Charles Strange's alleged injuries were too attenuated to constitute "concrete and particularized injury" as required by *Clapper*. *See Klayman*, 800 F.3d at 562 (Brown, J.) (internal quotation marks omitted). According to all three of our Circuit Judges, because plaintiffs had adduced no proof that "*their own* metadata was collected by the government" under the Program, they had not demonstrated a substantial likelihood of standing to pursue their claims. *Id.* at 562-63 (Brown, J.); *see also id.* at 565 (Williams, J.) ("[P]laintiffs lack direct evidence that records involving their calls have actually been collected."); *id.* at 569 (Sentelle, J., dissenting in part) ("[P]laintiffs never in any fashion demonstrate that the government is or has been collecting such records from their telecommunications provider."). Fortunately for plaintiffs, our Circuit's holding did not sound the death knell for their cause.

On September 16, 2015, plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange filed an uncontested Fourth Amended Complaint, joining as plaintiffs to the action VBNS subscribers J.J. Little and J.J. Little & Associates. *See* Fourth Am. Compl. Separately, and in an attempt to bolster their standing as Verizon Wireless subscribers, plaintiffs appended to their Complaint a document they claim shows that Verizon Wireless was "at all material times" participating in the Program. *See* Fourth Am. Compl. ¶ 47. I will begin by addressing plaintiffs' renewed arguments that Verizon Wireless was, and continues to be, a participant in the Program before turning to the merits of plaintiffs' alternative argument that the Little plaintiffs have standing to proceed.

Unfortunately for plaintiffs Klayman and Strange, I must conclude, in light of our Circuit's ruling in this case, that they have not adequately substantiated their injuries on remand. Plaintiffs appended to the Complaint a de-classified letter from the Department of Justice to the then-Presiding Judge of the FISC, Judge John D. Bates, regarding a "Compliance Incident Involving In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from . . . Cellco Partnership d/b/a Verizon Wireless." *See* Fourth Am. Compl. Ex. 1 [Dkt. #145-1]. Plaintiffs apparently interpret this document as confirmation that Verizon Wireless participated in the Program. Fourth Am. Compl. ¶¶ 47-48. The Government contends that it does no such thing. Gov't's Opp'n 17-18. While plaintiffs' suspicion is plausible, if not logical,[14] based on our Circuit Court's reasoning, I must agree with the Government that this document does not prove Verizon Wireless was ordered to turn over the metadata records of its customers. In fact, a Verizon spokesman suggested that the use of "Verizon Wireless" may simply be a vestige of "the government's practice to use broad language covering all of Verizon's entities in headings of such court orders . . . regardless of whether any specific part was required to provide information under that order." *See* Charlie Savage, *N.S.A. Used Phone Records Program to Seek Iran Operatives*, N.Y. Times, Aug. 12, 2015 (attached as Ex. 2 to Fourth Am. Compl.). As such, plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange have not shown a substantial likelihood that their telephony metadata

[14] Indeed, I went to great lengths in my December 2013 Opinion to debunk the notion that the NSA had omitted from the Program the single largest wireless carrier in the United States and in so doing had collected a universe of metadata so woefully incomplete as to undermine the Program's putative purpose. *See Klayman*, 957 F. Supp. 2d at 27. In my judgment, common sense still dictates that very conclusion regarding Verizon Wireless' participation in the Program.

was collected pursuant to the Program and therefore are not entitled to a preliminary injunction.

Quite the opposite, however, is true for the Little plaintiffs. The "irreducible constitutional minimum of standing" requires that plaintiffs "must have suffered an 'injury in fact'—an invasion of a legally protected interest which is . . . concrete and particularized." *Lujan*, 504 U.S. at 560. According to our Circuit Court, this demands evidence that "the [P]rogram targets plaintiffs." *See Klayman*, 800 F.3d at 567 (Williams, J.); *see also id.* at 563 (Brown, J.) (declining to find standing because "the facts marshaled by plaintiffs do not fully establish that their own metadata was ever collected"). The Little plaintiffs emphatically meet this hurdle. They aver in their Fourth Amended Complaint that "Little, for himself and by and through his law firm, J.J. Little & Associates, has been and continues to be a subscriber of Verizon Business Network Services for his firm J.J. Little & Associates, P.C." Fourth Am. Compl. ¶ 18. Their subscription has, moreover, been "continuous[]" since October 2011. Suppl. Decl. of J.J. Little ¶ 2 [Dkt. #152-1].[15] Because the Government has acknowledged that VBNS subscribers' call records were collected during a three-month window in which the Little plaintiffs were themselves VBNS subscribers, barring some unimaginable circumstances, it is overwhelmingly likely that their telephone metadata was indeed warehoused by the NSA. The Little plaintiffs, then, have pled facts wholly unlike those in *Clapper*. There is

[15] Indeed, as the Government defendants note in their brief, a district court found standing in a nearly identical set of circumstances in which the plaintiff "submitted specific testimonial evidence that it had received telephone service from VBNS 'since 2007' and continued to do so at the time it moved for injunctive relief. Gov't's Opp'n 19 n.9 (citing *ACLU v. Clapper*, No. 1:13-cv-3994 (S.D.N.Y.)).

no need to speculate that their metadata was targeted for collection, that the challenged Program was used to effectuate the metadata collection, that the FISC approved these actions, or that VBNS subscriber call records were indeed collected. Simply stated, *Clapper*'s "'speculative chain of possibilities' is, in this context, a reality." *ACLU v. Clapper*, 785 F.3d 787, 802 (2d Cir. 2015).

Given the strong presumption that the NSA collected, and warehoused, the Little plaintiffs' data within the past five years, these plaintiffs unquestionably have standing to enjoin any future queries of that metadata. The Government protests that there is "no evidence that the NSA has accessed records of [plaintiffs'] calls as a result of queries made under the 'reasonable, articulable suspicion' standard or otherwise." Gov't's Opp'n 20. To them, it is pure "conjecture" that "records of Plaintiffs' calls have been" or "will be" reviewed "during the remaining two months of the Section 215 program." Gov't's Opp'n 20. I wholeheartedly disagree. As I explained in my December 2013 Opinion, every single time the NSA runs a query to, for example, "detect foreign identifiers associated with a foreign terrorist organization calling into the U.S.," it must "analyze metadata for *every* phone number in the database by comparing the foreign target number against *all* of the stored call records to determine which U.S. phones, if any, have interacted with the target number." *Klayman*, 957 F. Supp. 2d at 28 (internal quotation marks omitted). The Second Circuit, not surprisingly, completely agrees. There, a court tasked with a substantially similar inquiry opined that the NSA "necessarily searches [plaintiffs'] records electronically, even if such a search does not

return [their] records for close review by a human agent." *See ACLU*, 785 F.3d at 802.[16] As the Second Circuit also points out, computerized searches "might lessen the intrusion," but they do not obviate it altogether. *Id.* A search remains a search regardless of how it is effectuated. If the Program is unlawful—and for the reasons discussed herein I believe it is substantially likely that it is—plaintiffs have suffered a concrete harm traceable to the challenged Program and redressable by a favorable ruling. For that reason, I find that the Little plaintiffs have "standing to object to the collection and review of their data."[17] *See id.*

Whether the Little plaintiffs have standing to challenge the *future* collection of their telephone metadata requires a separate analysis. The Government contends that the Little plaintiffs lack such standing because "there is no evidence before the Court that VBNS is currently a participating provider in the [Program]." Gov't's Opp'n 19. To them, "[a]n assumption that the NSA 'must be' collecting bulk telephony metadata from VBNS today because it did so for a three-month period in 2013 is precisely the sort of inference that the D.C. Circuit held in *Klayman* falls short of the certainty required under

---

[16] The analogy I used in my December 2013 Opinion remains instructive. Suppose one enters a hypothetical library to find each and every book citing *Battle Cry of Freedom* as a source. Suppose further that this goal has judicial pre-approval. *Battle Cry of Freedom* "might be referenced in a thousand books. It might be in just ten. It could be in zero. The only way to know is to check every book. At the end of a very long month, you are left with the 'hop one' results (those books that cite *Battle Cry of Freedom*), but to get there, you had to open every book in the library." *Klayman*, 957 F. Supp. 2d at 28 n.38.

[17] Brief mention must be made of the Government's argument that even if their data was collected, warehouse, and queried, the Little plaintiffs have failed to show a redressable injury. Specifically, the Government claims that plaintiffs lack standing because they have no "legally protected interest" in the collection and review of their telephone metadata. *See* Gov't's Opp'n 22. I held in my December 2013 Opinion that plaintiffs were likely to prove that the NSA's retrieval and querying process is indeed a Fourth Amendment search and decline to revisit that decision here. *See Klayman*, 957 F. Supp. 2d at 37.

[*Clapper*] to establish a plaintiff's standing in a case of this nature." Gov't's Opp'n 19. The Government's argument misconstrues what is required to establish standing in a case such as this. As I indicated *supra*, *Clapper* does not render Article III the enemy of every challenge to a classified surveillance program. Standing, in a post-*Clapper* world, remains an obstacle for the quixotic litigant, but is not a roadblock for the truly aggrieved. Rather, *Clapper* must be understood as it was unequivocally written: to stymie attenuated claims of harm. In that respect, our Circuit's holding in *Klayman* clearly abides. *See Klayman*, 800 F.3d at 566 (Brown, J.) (noting that Amnesty International's challenge in *Clapper* failed because plaintiffs "had no actual knowledge of the Government's § 1881a targeting practices nor could they even show that the surveillance program they were challenging even existed" (internal quotation marks omitted)); *see also id.* at 567 (Williams, J.) (likening plaintiffs' "assertion that NSA's collection must be comprehensive in order for the program to be effective" to the *Clapper* plaintiffs' speculative "assertions regarding the government's motive and capacity to target their communications"). According to our Circuit, a "substantial likelihood" of standing cannot rest on inferences about *which providers* participated in *this particular* Program. This proposition, however, does not mean that courts must abandon all common sense in determining the *scope* of that participation once concretely pled. Indeed, nothing in our Circuit Court's opinion precludes me from inferring, based on the NSA's past collection of VBNS subscriber data, that it continues to collect bulk telephony metadata from that *same* provider, pursuant to the *same* statutory authorization, to combat the *same* potential threats to our national security.

Indeed, common sense leads to that precise conclusion here. To start, I need not speculate that the Government continues to operate this Program. It has acknowledged as much. Potter Decl. ¶ 14. Proof that the Government *has* collected VBNS subscribers' metadata is, moreover, persuasive evidence that the threat of *ongoing* collection is not "chimerical." *See Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2345 (2014) (quoting *Steffel v. Thompson*, 415 U.S. 415, 459 (1973)). While the Government has not admitted that it continues to collect VBNS subscriber call records, its avowed need to combat terrorism makes it overwhelmingly likely that it does. According to Bryan Paarmann, Deputy Assistant Director of the Counterterrorism Division in the National Security Branch of the FBI, "[t]he threat environment confronting the United States has evolved" since this Court last opined. Paarmann Decl. ¶ 5 [Dkt. #150-6]. "Over the past two years the United States has confronted, and is still confronting, an increasing threat of attacks by individuals who act in relative isolation or in small groups." *Id.* This "increasingly diffuse threat environment" demands, under the FBI's logic, increased vigilance. *See* Paarmann Decl. ¶ 9; *see also id.* ¶ 11 ("[T]he current terrorist threat environment underscores the significance of this key ["contact chaining"] capability under the bulk telephony metadata program.").

The Government's position that VBNS may no longer be a participant in the Program is fundamentally at odds with its ever-escalating concerns of terrorist threats. By the Government's own admission, it is marshaling all available investigative tools to combat a threat it believes to be least as menacing as it was in 2013. *See* Paarmann Decl. ¶ 9. It defies common sense for defendants to argue, as they apparently do, that the

Government has chosen to omit from this breathtakingly broad metadata collection Program a provider that the Government surveilled in the past and that, presumably, has the infrastructure to continue assisting in that surveillance. In fact, it would make no sense whatsoever for the Government to use all available tools *except* VBNS call data to accomplish its putative goals. I am not alone in reaching this conclusion. The Second Circuit itself recently held that VBNS subscribers have standing to bring nearly identical claims because evidence that plaintiffs' "call records are indeed among those collected," made it unnecessary to speculate that the government "may in the future collect[] their call records." *ACLU*, 785 F.3d at 801. This is an imminent harm that is, once again, traceable to the challenged statute and remediable by a prospective injunction. Therefore, I find that the Little plaintiffs have standing to seek an order enjoining the future collection of their telephone metadata because they have shown a substantial likelihood that the NSA has collected and analyzed their telephone metadata and will continue to do so consistent with FISC opinions and orders. At the present time, no further amount of discovery is necessary to resolve the standing issue. Whether the Government's actions violate plaintiffs' Fourth Amendment rights is, of course, the province of the next section.

2. Plaintiffs are Likely to Succeed on the Merits of Their Fourth Amendment Claim.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. That right "shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the

place to be searched, and the persons or things to be seized." *Id.* A Fourth Amendment "search" occurs when "the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). In my December 2013 Opinion, I explained at length why both the indiscriminate bulk collection of telephony metadata and the analysis of that data each separately constitute a search within the meaning of the Fourth Amendment. *Klayman*, 957 F. Supp. 2d at 30-37. Neither the recent changes in the operation of the Program, nor the passage of the USA FREEDOM Act, has done anything to alter this analysis. The fact remains that the indiscriminate, daily bulk collection, long-term retention, and analysis of telephony metadata almost certainly violates a person's reasonable expectation of privacy.

Therefore, whether plaintiffs are entitled to preliminary injunctive relief at this stage turns on whether those searches are likely to be unreasonable, in light of intervening changes in the law. *See Kyllo*, 533 U.S. at 31 (whether a search has occurred is an "antecedent question" to whether a search was reasonable). Notwithstanding the Government's strong protestations, I conclude that plaintiffs will likely succeed in showing that the searches during this 180-day transition period still fail to pass constitutional muster.

a. Plaintiffs Will Likely Prove that the Searches Are Unreasonable.

The Fourth Amendment prohibits unreasonable searches. *See Samson v. California*, 547 U.S. 843, 848 (2006). Whether a search is reasonable depends on the totality of the circumstances. *Id.* Typically, searches not conducted pursuant to a warrant

based on the requisite showing of probable cause are "*per se* unreasonable." *Nat'l Fed'n of Fed. Emps.-IAM v. Vilsack*, 681 F.3d 483, 488-89 (D.C. Cir. 2012) (quoting *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010)). The Supreme Court, however, has recognized limited exceptions to this rule, including for situations in which "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (internal quotation marks omitted). Evaluating whether a warrantless, suspicionless search is reasonable under the "special needs" doctrine requires a court to balance the privacy interests implicated by the search against the governmental interest furthered by the intrusion. *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665-66 (1989).[18] Specifically, I must balance: (1) "the nature of the privacy interest allegedly compromised" by the search, (2) "the character of the intrusion imposed" by the

[18] Several categories of searches have been upheld under the "special needs" doctrine. Schools are permitted under certain circumstances to test students for drugs. *See Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls*, 536 U.S. 822, 838 (2002) (upholding urinalysis for all public school students participating in extracurricular activities); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 656 (1995) (upholding urinalysis for public school student athletes). The same is true for searches conducted by certain government employers. *See Von Raab*, 489 U.S. at 679 (upholding drug testing of Customs Service employees who applied for promotion to positions involving interdiction of illegal drugs or which required them to carry a firearm); *Willner v. Thornburgh*, 928 F.2d 1185, 1193-94 (D.C. Cir. 1991) (upholding urine tests of applicants for positions as attorneys at the Department of Justice). Officers may search probationers and parolees to ensure compliance with the rules of supervision. *See Griffin*, 483 U.S. at 880. And, in some cases, law enforcement may conduct suspicionless searches to prevent acts of terrorism in transportation centers. *See Cassidy v. Chertoff*, 471 F.3d 67, 87 (2d Cir. 2006) (upholding suspicionless searches of carry-on baggage and automobile trunks on Lake Champlain ferries); *MacWade v. Kelly*, 460 F.3d 260, 275 (2d Cir. 2006) (upholding searches of bags in New York City subway system). Suspicionless seizures have also been upheld under similar balancing analysis, including highway checkpoints designed to detect illegal entrants into the Unites States, *United States v. Martinez-Fuerte*, 428 U.S. 543, 567 (1976), and to catch intoxicated motorists, *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 455 (1990).

Government, and (3) "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them." *See Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls*, 536 U.S. 822, 830-34 (2002).

In my December 2013 Opinion, I held that the NSA's Bulk Telephony Metadata Program likely violated the Fourth Amendment because "plaintiffs [had] a substantial likelihood of showing that their privacy interests outweigh[ed] the Government's interest in collecting and analyzing bulk telephony metadata." *Klayman*, 957 F. Supp. 2d at 41. In opposition to plaintiffs' renewed motion for preliminary injunction, the Government argues that several developments since December 2013 have altered the special needs analysis such that plaintiffs are no longer likely to prevail. Gov't's Opp'n 33. For the following reasons, I do not agree.

i. Nature of the Privacy Interest

My analysis of the reasonableness of the searches at issue in this case begins with the nature of the privacy interest at stake. As I explained at length in my December 2013 Opinion, plaintiffs have a very significant expectation of privacy in an aggregated collection of their telephony metadata. *See Klayman*, 957 F. Supp. 2d at 32-37. When a person's metadata is aggregated over time, in this case five years, it can be analyzed to reveal "embedded patterns and relationships, including personal details, habits, and behaviors." Decl. of Prof. Edward W. Felten ¶¶ 24, 38-58 [Dkt. #22-1]. Recognizing that certain factors may diminish a person's otherwise robust privacy expectations, *see Willner v. Thornburgh*, 928 F.2d 1185, 1188 (D.C. Cir. 1991) ("[E]ven a current employee's 'expectation of privacy,' while 'reasonable' enough to make urine testing a

Fourth Amendment 'search,' can be so 'diminished' that the search is not 'unreasonable.'"), I consider this intrusion in the context of Americans' evolving interactions with mobile technology. Indeed, as of this year, 92 percent of American adults own a cellphone, 67 percent of whom own a so-called "smartphone" that enables them to, among other things, connect to the Internet. Lee Rainie & Kathryn Zickuhr, *Americans' Views on Mobile Etiquette*, *Chapter 1: Always on Connectivity*, Pew Research Center (Aug. 26, 2015), http://www.pewinternet.org/2015/08/26/chapter-1-always-on-connectivity/#fn-14328-1. Those who own such phones "often treat them like body appendages," as nine-in-ten cellphone owners carry their phones with them "frequently." *Id.* Smartphones, moreover, are not used merely for their basic communications functions, but rather "to help [owners] navigate numerous important life events," including for the sensitive purposes of online banking and researching health conditions. Aaron Smith, *U.S. Smartphone Use in 2015*, Pew Research Center (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/. The Government is quite right that these facets of mobile technology are not targeted by metadata collection. Nevertheless, Americans' constant use of cellphones for increasingly diverse and private purposes illustrates the attitude with which people approach this technology as a whole. Surely a person's expectation of privacy is not radically different when using his or her cellphone to make a call versus to check his or her bank account balance.

Furthermore, the attitude with which cellphone users approach their devices presents a dramatically different context than the contexts in which courts have upheld

"special needs" searches. Specifically, cellular phone technology does not present the same diminished expectation of privacy that typically characterizes "special needs" incursions. Take, for example, airports. In the context of air travel, courts have recognized that "society has long accepted a heightened level of security and privacy intrusion with regard to air travel." *Cassidy v. Chertoff*, 471 F.3d 67, 76 (2d Cir. 2006). Notably, Americans know that airports are discrete areas in which certain rights otherwise enjoyed are forfeited. *See id.* It is their choice to enter that space and, in so doing, to check certain rights at the door. Not so with cellphones. As already described, cellphones have become a constant presence in people's lives. While plaintiffs' privacy interests in their aggregated metadata may be somewhat diminished by the fact that it is held by third-party service providers, this is a *necessary* reality if one is to use a cellphone at all, and it is, therefore, simply not analogous to the context of voluntarily entering an airport. In this case, plaintiffs have asserted that the NSA's searches were a substantial intrusion on their privacy, and I have no reason to doubt that, nor to find that their privacy expectations should have been diminished given the context. Rather, I conclude that plaintiffs' privacy interests are robust.

ii. Character and Degree of Governmental Intrusion

Turning next to the character and degree of the Government's intrusion on plaintiffs' privacy interest, the Government avers that "[a]t this stage, the [P]rogram's potential for intrusion on Plaintiffs' privacy interests is minimal, and finite." Gov't's Opp'n 37. The Government first notes that the Program will no longer continue indefinitely but will end on November 29, 2015; therefore, any infringement is

necessarily limited in duration. *Id.* The Government next emphasizes that the new restrictions on queries—including that FISC authorization is now required before a query is conducted and that query results are now limited to "two hops"—significantly diminish the likelihood that plaintiffs' data will actually be reviewed. *Id.* Although I agree with the Second Circuit that there is now "a lesser intrusion on [plaintiffs'] privacy than they faced at the time this litigation began," *ACLU*, 785 F.3d at 826, I simply cannot agree with the Government's characterization of it as "minimal, and finite."

When considering whether a search is minimally or substantially intrusive, courts evaluate a variety of factors, including, *inter alia*, "the duration of the search or stop, the manner in which government agents determine which individual to search, the notice given to individuals that they are subject to search and the opportunity to avoid the search . . . as well as the methods employed in the search." *Cassidy*, 471 F.3d at 78-79 (citations omitted); *see also Willner*, 928 F.2d at 1189-90 (discussing as mitigating factors whether the person had "notice of an impending intrusion" and had a "large measure of control over whether he or she will be subject to" the search).

To say the least, the searches in this case lack most of these hallmarks of minimal intrusion. It is not, as an initial matter, a discrete or targeted incursion. To the contrary, it is a sweeping, and truly astounding program that targets millions of Americans arbitrarily and indiscriminately. To be sure, by designing a program that eliminates the need for agents to use discretion, the Government has reduced to zero the likelihood that metadata will be collected in a discriminatory fashion—a characteristic that the Supreme Court has suggested minimizes the privacy intrusion. *See, e.g.*, *United States v.*

Martinez-Fuerte, 428 U.S. 543, 559 (1976) (noting that roving patrols presented "a grave danger [of] unreviewable discretion," while fixed checkpoints reduce the scope of the intrusion because it "regularize[s]" enforcement). It is, however, absurd to suggest that the Constitution favors, or even tolerates, such extreme measures! To this Court's knowledge, no program has ever been upheld under the "special needs" doctrine that was not tailored, even if imperfectly, in some meaningful way.[19] Yet in this case the Government has made *no* attempt to tailor its program at all. *See Earls*, 536 U.S. at 852 (Ginsburg, J., dissenting) ("There is a difference between imperfect tailoring and no tailoring at all.").

Furthermore, although the intrusion plaintiffs now face may be "finite" in duration, it is certainly not "short." It is telling indeed that the searches and seizures upheld under the "special needs" doctrine have generally involved searches of significantly limited duration. *See, e.g.*, *Martinez-Fuerte*, 428 U.S. at 546-47 (upholding warrantless stops at a vehicle checkpoint where the average length of the stop was three

---

[19] Although not yet called upon to review an indiscriminate search of the breadth presented here, the Supreme Court has repeatedly hinted that it would be skeptical of a program that lacked sufficient tailoring. *See Earls*, 536 U.S. at 844 (Ginsburg, J., dissenting) ("Those risks [of illegal drug use], however, are present for *all* schoolchildren. *Vernonia* cannot be read to endorse invasive and suspicionless drug testing of all students upon any evidence of drug use, solely because drugs jeopardize the life and health of those who use them."); *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000) ("[T]he Fourth Amendment would almost certainly permit *an appropriately tailored roadblock* set up to thwart an imminent terrorist attack. The exigencies created by these scenarios are far removed from the circumstances under which authorities might simply stop cars as a matter of course to see if there just happens to be a felon leaving the jurisdiction.") (emphasis added); *see also Cassidy*, 471 F.3d at 80-81 (recognizing the "legitimate concern" that the government's power to conduct suspicionless searches may be limitless given the threat of terrorism is "omnipresent" but finding that concern not implicated "where the government has imposed security requirements only on the nation's largest ferries after making extensive findings about the risk these vessels present in relation to terrorism and . . . the scope of the searches is rather limited").

to five minutes). In contrast, under this Program, the NSA collects data on a *daily basis* and maintains the metadata gathered from those daily searches for *five years*. Moreover, though the weeks remaining in the Program may seem relatively short given that the previous timeframe was *indefinite*, this reduced period still significantly dwarfs the duration of the intrusion in all "special needs" cases of which this Court is aware. With respect to the institution of new procedures for authorizing database queries and the new limitations on the extent of the records returned for review, while these new methods of searching may further mitigate the privacy intrusion that occurs when the NSA queries and analyzes metadata, there continues to be *no minimization procedures* applicable at the collection stage. *See* Oct. 11, 2013 Primary Order at 3-4 (requiring the Order's recipients to turn over all of their metadata without limit).

Finally, far from Americans being put on notice of the Bulk Telephony Metadata Program such that they could choose to avoid it, the Program was, and continues to be, shrouded in secrecy. This may, of course, be practically necessary for the Program to be effective, but it nevertheless increases the level of the privacy intrusion. *See, e.g.*, *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 657 (1995) (analogizing students who choose to participate in athletics to "adults who choose to participate in closely regulated industry"); *Von Raab*, 489 U.S. at 675 n.3 ("When the risk is the jeopardy to hundreds of human lives . . . that danger *alone* meets the test of reasonableness, so long as the search is conducted . . . with reasonable scope and the passenger has been given advance notice of his liability to such a search so that he can avoid it by choosing not to travel by air.") (internal quotation marks omitted); see *also Willner*, 928 F.2d at 1190 ("[T]he applicant's

knowledge of what will be required, and when, affects the strength of his or her interest."). In sum, despite changes to the Program, the Government is still, in effect, asking this Court to sanction a dragnet of unparalleled proportions.

iii. Nature of Government's Interest and Efficacy

Having found that the first two factors militate in plaintiffs' favor, I must finally consider whether the nature of the Government's interest and the efficacy of the Program in meeting its goals are, nevertheless, substantial enough to tip the balance in the Government's favor. As I stated in my December 2013 Opinion, I agree with the Government that the purpose of "identifying unknown terrorist operatives and preventing terrorist attacks" is an interest of the highest order that goes beyond regular law enforcement needs. *Klayman*, 957 F. Supp. 2d at 39 (internal quotation marks omitted). More specifically, though, I found that the Government's true interest was in identifying and investigating imminent threats *faster* than would be otherwise possible.[20] *Id.* at 39-40. Given that the Program's end is only several weeks away, the Government now also argues that the transition period meets the particular need of avoiding the creation of "an intelligence gap in the midst of the continuing terrorist threat." Gov't's Opp'n 34. While an "intelligence gap"—however amorphous its contours—could be significant in theory, the Government has not sufficiently defined it to date to warrant that characterization.

[20] This emphasis remains today, especially in light of the evolving nature of the terrorist threat. *See* Paarmann Decl. ¶ 9 ("Because of this increasingly diffuse threat environment, the availability of all investigative tools that permit the [Government] to detect and respond to terrorist threats quickly, has become increasingly important."); *see also* Gov't's Opp'n 35 ("Analysis of telephony metadata to *quickly* detect contacts of known or suspected terrorists is an important component of the Government's counter-terrorism arsenal.").

But even if it had, proffering a significant special need is not the end of this Court's inquiry. *See City of Indianapolis v. Edmond*, 531 U.S. 32, 42 (2000) ("[T]he gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose."). Rather, I must also evaluate the efficacy of the searches at issue in meeting this need. *See Cassidy*, 471 F.3d at 85-86. To date, the Government has still not cited a single instance in which telephone metadata analysis actually stopped an imminent attack, or otherwise aided the Government in achieving any time-sensitive objective.[21] Although the Government is not required to adduce a specific threat in order to demonstrate that a "special need" exists, *see Earls*, 536 U.S. at 835-36, providing this Court with examples of the Program's success would certainly strengthen the Government's argument regarding the Program's efficacy. This is especially true given that the Program is not designed for detection *and deterrence* like most other programs upheld under the "special needs" doctrine. Indeed, most warrantless searches upheld under the "special needs" doctrine boast *deterrence* as a substantial Governmental interest. For example, screening passengers' bags before allowing them to board a ferry may rarely detect an actual attempt to board with

[21] In the Government's most recent declaration regarding the need for the Program, it states that given "an increasing threat of attacks by individuals who act in relative isolation or in small groups," Paarmann Decl. ¶ 5, including at the encouragement of the Islamic State of Iraq and the Levant and al-Qaeda, "the availability of all investigative tools that permit the FBI and its partners to detect and respond to terrorist threats quickly, has become increasingly important," *id.* at ¶ 9. With respect to the Bulk Telephony Metadata Program, the Government states: "Information gleaned from NSA analysis of telephony metadata *can be* an important component of the information the FBI relies on to identify and disrupt threats," *id.* at ¶ 10 (emphasis added), it "*can provide* information earlier than other investigative methods and techniques," and "earlier receipt of this information *may advance* an investigation and contribute to the disruption of a terrorist attack that, absent the metadata tip, the FBI might not have prevented in time," *id.* at ¶ 12 (emphasis added). Not exactly confidence inspiring!

dangerous substances or devices, but may nevertheless be deemed reasonable because of its deterrent effect. *See Cassidy*, 471 F.3d at 85-86; *see also Von Raab*, 489 U.S. at 675 n.3 ("Nor would we think, *in view of the obvious deterrent purpose of these searches*, that the validity of the Government's airport screening program necessarily turns on whether significant numbers of putative air pirates are actually discovered by the searches." (emphasis added)). The same cannot be said of this Program. Because secrecy is the hallmark of the Program, the deterrent value is effectively zero and its efficacy can only be measured by its ability to detect, and thereby prevent, terrorist attacks.

Nevertheless, instead of providing this Court with specific examples of the Program's success, the Government makes the bootstrap argument that the enactment of the USA FREEDOM Act confirms the importance of this Program to meeting the Government's special needs, Gov't's Opp'n 34, and suggests that this Court should defer to that judgment, *see id.* at 35 n.24. Please! I recognize that my duty to evaluate the efficacy of this Program is "not meant to transfer from politically accountable officials to the courts the decision as to which among reasonable alternative law enforcement techniques should be employed to deal with a serious public danger." *See Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 453 (1990). Nonetheless, while "the choice among such reasonable alternatives remains with the governmental officials," *id.* at 453-54, I must still determine whether the Program is reasonably effective in accomplishing its goals, even if not optimally so, *see Cassidy*, 471 F.3d at 85-86 (noting that a court's task is not to determine whether a particular program is "optimally effective, but whether it [is] reasonably so"). This is a conclusion I simply cannot reach given the continuing lack

of evidence that the Program has ever actually been successful as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism. Accordingly, having determined that the Government has proffered a "special need," but done nothing to abate my lingering doubts about whether the Bulk Telephony Metadata Program is reasonably effective at meeting this need, I find this factor weighs in the Government's favor, but only to a limited extent.

In conclusion, I find that plaintiffs are substantially likely to demonstrate that they have a robust privacy interest in their aggregated metadata and that the intrusion thereon by the Bulk Telephony Metadata Program is substantial. Against these factors, which weigh heavily in plaintiffs' favor, I further find that, although the Government has proffered a compelling "special need" of quickly identifying and investigating potential terror threats, plaintiffs will likely be able to show that the Program is not reasonably effective at meeting this need. Therefore, plaintiffs will likely succeed in showing that the Program is indeed an unreasonable search under the Fourth Amendment.

B. Plaintiffs Will Suffer Irreparable Harm Absent Injunctive Relief.

As I have discussed at length, plaintiffs have demonstrated that they are substantially likely to succeed on their claim that the Government is actively violating the rights guaranteed to them by the Fourth Amendment. Because "[i]t has long been established that the loss of constitutional freedoms, 'for even minimal periods of time, unquestionably constitutes irreparable injury,'" *Mills v. District of Columbia*, 571 F.3d 1304, 1312 (D.C. Cir. 2009) (quoting *Elrod v. Burns*, 427 U.S. 347, 373 (1976)), the

Little plaintiffs have adequately demonstrated irreparable injury. As such, it makes no difference that this violation now has a foreseeable end.[22]

C. The Public Interest and Potential Injury to Other Interested Parties Both Weigh in Plaintiffs' Favor.

The final factors I must consider in weighing plaintiffs' entitlement to preliminary injunctive relief are the balance of the equities and the public interest. *See Sottera*, 627 F.3d at 893. As an initial matter, I emphasize the obvious: "enforcement of an unconstitutional law is always contrary to the public interest." *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013); *see also Hobby Lobby Stores, Inc. v. Sebelius*, 723 F.3d 1114, 1145 (10th Cir. 2013) ("[I]t is always in the public interest to prevent the violation of a party's constitutional rights." (internal quotation marks omitted)), *aff'd sub nom. Burwell v. Hobby Lobby Stores, Inc.*, 134 S. Ct. 2751 (2014); *Melendres v. Arpaio*, 695 F.3d 990, 1002 (9th Cir. 2012) (same); *Am. Freedom Def. Initiative v. Wash. Metro. Area Transit Auth.*, 898 F. Supp. 2d 73, 84 (D.D.C. 2012) (same); *Nat'l Fed'n of Fed. Emps. v. Carlucci*, 680 F. Supp. 416, 435 (D.D.C. 1988) ("[T]he public interest lies

---

[22] Against this presumption, the Government incredibly argues that the Little plaintiffs' claim of irreparable harm is necessarily undercut by their more than two-year delay in joining this suit. Gov't's Opp'n 24 n.12. Come on! While delay in filing may suggest the proffered harm is not truly irreparable, late filing alone is not a sufficient basis for denying a preliminary injunction. *See Gordon v. Holder*, 632 F.3d 722, 724 (D.C. Cir. 2011) ("[A] delay in filing is not a proper basis for denial of a preliminary injunction."). In this case, I do not find the two-year delay to be significant. Although the Government emphasizes the "personal" nature of Fourth Amendment rights, *see* Gov't's Opp'n 29, it was certainly reasonable for the Little plaintiffs to perceive that their rights would ultimately be vindicated by other similarly-situated plaintiffs—the expectation of privacy in their telephony metadata is identical and the searches thereof were reasonably inferred to be the same. *Cf. Cooper v. Aaron*, 78 S. Ct. 1401 (1958) (holding that Arkansas state officials were bound by the Supreme Court's prior decision that racial segregation in public schools was unconstitutional in a case involving four different states that employed a similar system). Until our Circuit Court's decision regarding standing, there was little reason for the Little plaintiffs to believe they were uniquely positioned to challenge the Program.

in enjoining unconstitutional searches."). Given my finding that plaintiffs are likely to succeed on the merits of their Fourth Amendment claim, the public interest weighs heavily in their favor.

Undaunted, the Government argues that the public interest actually counsels *against* granting a preliminary injunction in this case because of the public's strong interest in maintaining an ability to *quickly* identify and investigate terrorist threats. *See* Gov't's Opp'n 45. Indeed, the Government goes one step further by arguing that *United States v. Oakland Cannabis Buyers' Cooperative*, 532 U.S. 483 (2001), requires this Court to defer to Congress's "determination" that continuing the Program during the 180-day transition period is the best way to protect the public's interest.[23] *See* Gov't's Opp'n 38. Not quite! Congress did not *explicitly* authorize a continuation of the Program. Rather, it artfully crafted a starting date for the prohibition of the Program that would enable the Government to confidentially seek FISC authorization to continue the Program for the 180-day transition period and free the Members of Congress from having to vote for an *explicit* extension of the Program. *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 109, 128 Stat. 268, 276 (2015). Moreover, while *Oakland* "prohibits a district court from second-guessing Congress's lawful prioritization of its policy goals," it in no way limits a court from evaluating "the lawfulness of Congress's means of achieving those priorities." *Gordon*, 721 F.3d at 652-53; *see also Vilsack*, 681 F.3d at 490 (noting

[23] In *Oakland*, the district court enjoined the defendant cooperative from distributing marijuana except in cases of medical necessity. In overturning the appeals court decision affirming this injunction, the Supreme Court found that the district court could not ignore Congress's determination, as expressed through legislation, that marijuana has no medical benefits warranting its limited distribution. *Oakland*, 532 U.S. at 496-99.

that "[d]eference is never blind" and "the constitutional question is distinct from policy questions involving otherwise constitutional administrative judgments about how best to operate a program"). Congress, of course, is *not* permitted to prioritize any policy goal over the Constitution. *Gordon*, 721 F.3d at 653. Nor am I! *See Marbury v. Madison*, 5 U.S. 137, 180 (1803) ("Thus, the particular phraseology of the constitution of the United States confirms and strengthens the principle, supposed to be essential to all written constitutions, that a law repugnant to the constitution is void; and that *courts,* as well as other departments, are bound by that instrument.").[24] This Court simply cannot, and will not, allow the Government to trump the Constitution merely because it suits the exigencies of the moment.

This Court's vigilance in upholding the Constitution against encroachment is, of course, especially strong in the context of the Fourth Amendment. Indeed, the Judiciary has long recognized that:

> Moved by whatever momentary evil has aroused their fears, officials—perhaps even supported by a majority of citizens—may be tempted to conduct searches that sacrifice the liberty of each citizen to assuage the perceived evil. But the Fourth Amendment rests on the principle that a true balance between the individual and society depends on the recognition of "the

[24] For this reason, it is unsurprising that the Government has not proffered a single case in which a plaintiff who was likely to prevail on the merits of a constitutional claim was denied a preliminary injunction because of the gravity of the public interest. In *In re Navy Chaplaincy*, 697 F.3d 1171 (D.C. Cir. 2012), our Circuit was reviewing the denial of a preliminary injunction where the District court concluded that although plaintiffs had shown irreparable harm, they were *not* likely to succeed on the merits of their First Amendment claims and the public interest and balance of the equities weighed against them. *Id.* at 1178-79. Similarly, in *Davis v. Billington*, 76 F. Supp. 3d 59 (D.D.C. 2014), the District court denied a request for preliminary injunction where all the preliminary injunction factors weighed against plaintiff, including his likelihood of success on the merits of his constitutional claim. *Id.* at 68-69.

> right to be let alone—the most comprehensive of rights and the right most valued by civilized men."

New Jersey v. T.L.O., 469 U.S. 325, 361-62 (1985) (quoting *Olmstead v. United States,* 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)). To be sure, the very purpose of the Fourth Amendment would be undermined were this Court to defer to Congress's determination that individual liberty should be sacrificed to better combat today's evil.

The Government concludes by discussing at length the negative impact an injunction in this case would have on the Program as a whole, including that the *immediate* cessation of collection of or analytic access to metadata associated with plaintiffs' telephone numbers, if ordered, would require the NSA to terminate the Program altogether. Gov't's Opp'n 41-45. This would be the case, the Government argues, for several reasons. First, the NSA would need to obtain information regarding plaintiffs' telephone numbers and would need to be granted FISC authorization to access the database for the purpose of complying with this Court's order. Gov't's Opp'n 41-42. Beyond these preliminary steps, it would take an undetermined amount of time to develop the technical means to comply with the Court's order, including figuring out how to ensure no new metadata relating to plaintiffs' records is added to the database and how to discontinue analytic access to any metadata relating to plaintiffs' records that is currently in the database. Gov't's Opp'n 43-44. Unfortunately for the Government, this Court does not have much sympathy for these last minute arguments. The Government was given unequivocal notice that it may be required to undertake steps of this nature in my December 2013 Opinion granting plaintiffs' request for a preliminary injunction.

Indeed, I expressly warned against any future request for delay stating, "I fully expect that during the appellate process, which will consume at least the next six months, the Government will take whatever steps necessary to prepare itself to comply with this order when, and if, it is upheld." *Klayman*, 957 F. Supp. 2d at 44. Given that I significantly under-estimated the duration of the appellate process, the Government has now had *over twenty-two months* to develop the technology necessary to comply with this Court's order. To say the least, it is difficult to give meaningful weight to a risk of harm created, in significant part, by the Government's own recalcitrance.

CONCLUSION

With the Government's authority to operate the Bulk Telephony Metadata Program quickly coming to an end, this case is perhaps the last chapter in the Judiciary's evaluation of this particular Program's compatibility with the Constitution. It will not, however, be the last chapter in the ongoing struggle to balance privacy rights and national security interests under our Constitution in an age of evolving technological wizardry. Although this Court appreciates the zealousness with which the Government seeks to protect the citizens of our Nation, that same Government bears just as great a responsibility to protect the individual liberties of those very citizens.

Thus, for all the reasons stated herein, I will grant plaintiffs J.J. Little and J.J. Little & Associates' requests for an injunction[25] and enter an order consistent with this Opinion that (1) bars the Government from collecting, as part of the NSA's Bulk

[25] For reasons stated at the outset, this relief is limited to these plaintiffs. I will deny the motion as it relates to plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange.

Telephony Metadata Program, any telephony metadata associated with these plaintiffs' Verizon Business Network Services accounts and (2) requires the Government to segregate any such metadata in its possession that has already been collected.[26] In my December 2013 Opinion, I stayed my order pending appeal in light of the national security interests at stake and the novelty of the constitutional issues raised. I did so with the optimistic hope that the appeals process would move expeditiously. However, because it has been almost two years since I first found that the NSA's Bulk Telephony Metadata Program likely violates the Constitution and because the loss of constitutional freedoms for even one day is a significant harm, *see Mills*, 571 F.3d at 1312, I will not do so today.

RICHARD J. LEON
United States District Judge

[26] Although it is true that granting plaintiffs the relief they request will force the Government to identify plaintiffs' phone numbers and metadata records, and then subject them to otherwise unnecessary individual scrutiny, *see* Gov't's Opp'n 41-42, that is the only way to remedy the constitutional violations that plaintiffs are substantially likely to prove on the merits.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KLAYMAN et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	**Civil Action No. 13-0851 (RJL)**
	)	
OBAMA et al.,	)	
	)	
Defendants.	)	

ORDER
(November 9, 2015)

For the reasons set forth in the Memorandum Opinion entered this date, it is hereby

ORDERED that plaintiffs' Renewed Motion for Preliminary Injunction [Dkt. #149] is **GRANTED** as to plaintiffs J.J. Little and J.J. Little & Associates, P.C. and **DENIED** as to plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange; it is further

ORDERED that the Government:

(1) is barred from collecting, as part of the NSA's Bulk Telephony Metadata Program, any telephony metadata associated with J.J. Little and J.J. Little & Associates, P.C. Verizon Business Network Services telephone subscriptions; and

(2) must segregate out all such metadata already collected from any future searches of its metadata database.

SO ORDERED.

RICHARD J. LEON
United States District Judge

[ORAL ARGUMENT NOT YET SCHEDULED]

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

LARRY KLAYMAN, *et al.*,	
Plaintiffs-Appellees,	
v.	No. 15-5307
BARACK H. OBAMA, *et al.*,	[Civil Action Nos. 13-CV-0851 (RJL) 13-CV-0881 (RJL)]
Defendants-Appellants.	

EMERGENCY MOTION FOR STAY PENDING APPEAL AND FOR IMMEDIATE ADMINISTRATIVE STAY

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

CHANNING D. PHILLIPS
United States Attorney

DOUGLAS N. LETTER
H. THOMAS BYRON III
(202) 616-5367
CATHERINE H. DORSEY
(202) 514-3469
Attorneys, Appellate Staff
Civil Division, Room 7236
Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

INTRODUCTION AND SUMMARY

On November 9, 2015, the district court entered a preliminary injunction that requires the government to cease collection and analysis of the telephony metadata of certain plaintiffs (the Little plaintiffs) under the government's Section 215 program for collection of bulk telephony metadata. As the government explained to the district court, however, the technical steps necessary to comply with such a targeted injunction would require at least several weeks to complete. Absent a stay, therefore, immediate compliance with the district court's injunction would effectively require the abrupt termination of that important counter-intelligence program, as explained below. Such a result is contrary to Congress's judgment that the Section 215 program should instead end only after a transition period (ending less than three weeks from now) to avoid a gap in intelligence collection that could harm national security. As the Second Circuit recently held, that considered legislative decision should be respected and not overturned on the basis of uncertain constitutional claims that will be rendered moot in a matter of weeks. *ACLU* v. *Clapper*, 2015 WL 6516757, at *8-9 (2d Cir. Oct. 29, 2015).

The government immediately sought a stay of the injunction, which the district court denied today. Accordingly, the government asks this Court for a stay pending appeal, and for an immediate administrative stay pending this Court's resolution of this motion. (If neither type of order is granted by the Court, we move for a stay of at least ten days to allow the government to seek relief from the Supreme Court, if

authorized by the Solicitor General.) The government respectfully asks that this Court enter a stay as early as possible; otherwise, the government could be forced to abruptly terminate an important counter-intelligence program *in toto*, while it continues a burdensome and technically difficult process to prevent collection of and analytic access to any metadata associated with only the Little plaintiffs. Opposing counsel Larry Klayman has requested that we inform the Court that plaintiffs oppose the government's motion and wish to be heard by this Court before it considers whether to grant any administrative stay pending appeal.

This case arises out of a challenge to the Section 215 bulk telephony-metadata program, an important intelligence-gathering program designed to detect and prevent terrorist attacks, which is authorized by orders issued by the Foreign Intelligence Surveillance Court. Under that program, the government acquires business records from certain telecommunications companies, in bulk, that contain telephony metadata reflecting the time, duration, dialing and receiving numbers, and other information about telephone calls, but that do not identify the individuals involved in, or the content of, the calls. Pursuant to new legislation, that program will end in less than three weeks when the government transitions to a new intelligence program based on targeted rather than bulk collection of telephony metadata.

Despite the imminent termination of the program, the district court enjoined the government from collecting certain plaintiffs' telephony metadata, concluding that those plaintiffs were likely to succeed in showing that the program violates the Fourth

Amendment. That decision is contrary to the Second Circuit's recent decision, which denied an injunction against the government's Section 215 bulk collection program because, regardless of whether the program was lawful prior to passage of the USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268 (2015), Congress authorized the continuation of the program during the 180-day transition period to the new intelligence program. *See generally Clapper*, 2015 WL 6516757. The district court decision is also contrary to the conclusions of numerous district courts and judges of the Foreign Intelligence Surveillance Court who have upheld the program's constitutionality. The district court's issuance of an injunction was also in error because plaintiffs lack standing to obtain any relief, have shown no irreparable injury, have little chance of succeeding on the merits, and lose the balancing of equities in favor of Congress's considered judgment that continued operation of the Section 215 program is necessary during the transition period to avoid an intelligence gap.

Absent a stay, complying with the district court's preliminary injunction, which is purportedly limited to data concerning the Little plaintiffs, would effectively require the government to terminate the Section 215 program prematurely, creating an intelligence gap during the transition and thereby impairing the government's ability to timely gather intelligence that the government relies upon to identify and disrupt terrorist threats. Congress, however, made a considered judgment through a reasonable balancing of the various public interests associated with the program, including as to how to bring the program to an orderly end, consistent with national

security concerns. By entering an injunction, the district court improperly rejected the balance that Congress has struck in a statute.

Indeed, where a single district judge prohibits enforcement of a statute on constitutional grounds, as the district court here has done, the government is almost invariably entitled to a stay pending appeal. *See Bowen* v. *Kendrick*, 483 U.S. 1304, 1304-05 (1987) (Rehnquist, J., in chambers); *Walters* v. *National Ass'n of Radiation Survivors*, 468 U.S. 1323, 1324 (1984) (Rehnquist, J., in chambers); *cf. Maryland* v. *King*, 133 S.Ct. 1, 3 (2012) (Roberts, C.J., in chambers) ("[A]ny time a State is enjoined by a court from effectuating statutes enacted by representatives of its people, it suffers a form of irreparable injury.").

STATEMENT

1. The district court's preliminary injunction prohibits the government from collecting the business records of telecommunications service providers containing telephony metadata concerning the calls of plaintiffs J.J. Little and his law firm, J.J. Little & Associates, P.C. (collectively, the "Little plaintiffs"), as part of the bulk telephony-metadata program that the government operates under the authority of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1810. As the government explained to the district court, the only practicable way for the NSA to comply with the court's preliminary injunction is immediately to cease *all* collection and queries of metadata under the Section 215 program because the technical steps required to prevent further collection and segregation of the metadata associated with the Little plaintiffs would

take the NSA at least several weeks to complete. *See* Potter Decl. (Dkt. # 150-4) ¶¶ 20-27 (*see* Attachment D).

Pursuant to Section 215 of the USA PATRIOT Act, codified at 50 U.S.C. § 1861, the United States, for a few more weeks, operates a telephony-metadata intelligence-gathering program as part of its efforts to combat international terrorism. Companies that provide telecommunications services create and maintain records containing telephony metadata for the companies' own business purposes, such as billing and fraud prevention, and they provide those business records to the federal government in bulk pursuant to court orders issued under Section 215. The data obtained under those court orders do not include information about the identities of individuals; the content of the calls; or the name, address, financial information, or cell site locational information of any telephone subscribers. The government uses the Section 215 telephony-metadata program as a tool to facilitate counterterrorism investigations – specifically, to ascertain whether international terrorist organizations are communicating with operatives in the United States.

As the FBI has explained, the United States faces an "increasingly diffuse threat environment," Paarmann Decl. ¶ 9 (Dkt. # 150-6) (*see* Attachment E), in which the Islamic State of Iraq and the Levant and other foreign terrorist organizations encourage small-scale attacks against the United States that can be planned and carried out more quickly than large-scale attacks, yet can be more difficult to detect. *Id.* ¶¶ 5-7. Although various sources of information can each be used to provide separate and

independent indications of potential terrorist activity, the best and most timely analysis occurs when intelligence information obtained from all of those sources can be considered together to compile as complete a picture as possible of that threat. *Id.* ¶ 10. Information gleaned from NSA analysis of telephony metadata can be an important component of the information the FBI relies on to dependably execute its threat detection and prevention responsibilities. *Id.*

Consistent with the President's objective to replace the Section 215 program with a targeted collection program that provides greater privacy protections, just several months ago Congress enacted the USA FREEDOM Act. The Act prohibits the government from conducting the bulk collection of telephony metadata under Section 215 as of November 29, 2015, and provides for a new system of targeted production of call detail records. *See* USA FREEDOM Act §§ 101, 103.

Congress provided for a six-month transition period by delaying for 180 days the effective date of the prohibition on bulk collection under Section 215, and also the corresponding implementation date of the new regime of targeted production under the statute. USA FREEDOM Act § 109. The design and effect of delaying the prohibition on bulk collection preserves the government's intelligence capabilities by permitting the Section 215 program to continue for six months while the NSA creates the technical ability to operate under the new model of targeted production. *See* 161 Cong. Rec. S3439-40 (daily ed. June 2, 2015) (statement of Sen. Leahy); 161 Cong. Rec. S3275 (daily ed. May 22, 2015) (statement of Sen. Leahy). As the government

explained to Congress, the implementation of the new production regime requires a six-month transition period for the government to provide to telecommunications companies "the technical details, guidance, and compensation to create a fully operational" new querying model. *Id.*

Pursuant to the authority conferred by the USA FREEDOM Act, the government applied to the Foreign Intelligence Surveillance Court for authorization to resume the Section 215 bulk-collection program during the transition period, which that court granted. *See Primary Order, In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, No. BR 15-75, 2015 WL 5637563, at *5 (FISA Ct. June 29, 2015) (holding that the USA FREEDOM Act explicitly authorized the government to continue the Section 215 bulk telephony-metadata program during the 180-day transition).

After the transition period ends, no further bulk collection of telephony metadata will occur under Section 215, and analytic access to previously collected metadata will also cease – the data will not be used for intelligence or law-enforcement purposes, and will not be disseminated. Further, the underlying data will be destroyed as soon as possible.[1] Potter Decl. ¶¶ 15-17; *ODNI*, *Statement by the ODNI on Retention of Data Collected Under Section 215 of the USA PATRIOT Act*, July 27,

[1] If permitted by order of the Foreign Intelligence Surveillance Court, the government will retain technical access for a three-month period to ensure the proper function of the replacement program and any additional retention required for compliance with the government's preservation obligations as a civil litigant.

2015, http://www.dni.gov/index.php/newsroom/press-release/210-press-release-2015/1236-statement-by-the-odni-on-retention-of-data-collected-under-section-215-of-the-usa-patriot-act.

2. Plaintiffs previously moved for a preliminary injunction prohibiting bulk collection of metadata, which the district court granted. The district court concluded that two plaintiffs (Klayman and Strange) had standing to challenge the Section 215 program. As to the merits, the district court concluded that the Section 215 program constitutes a "search" within the meaning of the Fourth Amendment. The district court determined that *Smith* v. *Maryland*, 442 U.S. 735 (1979), which held that individuals have no reasonable expectation of privacy in the telephone numbers they dial, is not controlling. *Klayman* v. *Obama*, 957 F. Supp. 2d 1, 32-37 (D.D.C. 2013). The court next held that such a search does not meet the test of reasonableness under the Fourth Amendment, because the program's intrusion on plaintiffs' "significant expectation of privacy" outweighs its contribution to national security (as the court assessed it). *Id.* at 39-42.

The court also held that plaintiffs Klayman and Strange had demonstrated irreparable injury because "the loss of constitutional freedoms, 'for even minimal periods of time, unquestionably constitutes irreparable injury,'" *Klayman*, 957 F. Supp. 2d at 42, and that providing relief to those two plaintiffs alone would not harm the public, *id.* at 43. "[I]n light of the significant national security interests at stake,"

however, and the perceived novelty of the constitutional issues, the court stayed its injunction pending the government's appeal. *Id.*

3. This Court vacated the district court's preliminary injunction and remanded the case for further proceedings. *Obama* v. *Klayman*, 2015 WL 5058403, at *2 (D.C. Cir. Aug. 28, 2015) (per curiam). Two of the judges on the panel held that plaintiffs had not demonstrated standing because they had not adequately established that the government had collected call records from their carrier, Verizon Wireless. *Id.* at *8 (Williams, J.); *id.* at *10 (Sentelle, J.).

4. On remand, plaintiffs added the Little plaintiffs, who are alleged to have been subscribers of Verizon Business Network Services, Inc. "[a]t all material times." Plaintiffs renewed their motion for a preliminary injunction against the Section 215 program.

5. The district court yesterday entered an injunction barring the government from collecting any telephony metadata associated with the Little plaintiffs and requiring the government to "segregate out all such metadata already collected from any future searches of its metadata database." Order of Nov. 9, 2015 (Dkt. # 159) (*see* Attachment B). Although the injunction nominally extends relief only to the Little plaintiffs, the district court recognized that its injunction could require the government to abruptly terminate the Section 215 program, given that the government would otherwise need to undertake a burdensome and technically

difficult process to cease collection and analytic access as to only the Little plaintiffs. Opinion of Nov. 9, 2015 (Dkt. # 158) ("Slip Op.") at 41-42 (*see* Attachment A).

The district court relied on its earlier opinion to conclude that the bulk collection of telephony metadata under Section 215 constitutes an unconstitutional search within the meaning of the Fourth Amendment. Slip Op. at 26. Although the district court conceded that the government's intrusion on that privacy interest is "finite," given the imminent termination of the Section 215 program, the court nevertheless concluded that the intrusion was not sufficiently limited to uphold it under the "special needs" doctrine. Slip Op. at 32-33.

Finally, the district court concluded that both plaintiffs and the public will suffer irreparable harm to their privacy interests absent injunctive relief. Slip Op. at 37-39. The court rejected the government's argument that the public interest weighs against an injunction and that the court should defer to Congress's judgment to continue the Section 215 program during the transition period, stating that "Congress did not *explicitly* authorize a continuation of the Program." Slip Op. at 39.

6. That same day, the government moved for a stay, which the district court denied today.

ARGUMENT

This Court should grant a stay pending appeal (and, at a minimum, an administrative stay pending the Court's resolution of this motion) to prevent the unwarranted and disruptive termination of the government's Section 215 program

during the final weeks of the transition provided for by Congress. Particularly where the bulk collection program that plaintiffs challenge will expire in less than three weeks, and Congress has already determined that it is necessary and appropriate to continue that program until the government can put into operation the new targeted system of collection, the equities weigh decisively in favor of a stay. Indeed, the Second Circuit recently declined to enjoin the Section 215 program given Congress's considered judgment to continue that program during the transition period and that any constitutional claims would soon be rendered moot by the program's termination on November 29, 2015. *Clapper*, 2015 WL 6516757, at *6-9.

A. In Light of the Immediate Harm to the Government and the Public, the Balance of Harms Warrants a Stay.

Absent a stay, the government is prohibited from collecting under Section 215 or conducting analytic queries of any business records reflecting telephony metadata associated with the Little plaintiffs' Verizon Business Network Services accounts. As explained in the attached NSA declaration, immediate compliance with the district court's injunction would require the government to cease *all* bulk collection and queries of telephony-metadata under the Section 215 program. The Section 215 program, however, is an important component of the government's counter-terrorism arsenal. Compelling the termination of that program before the transition to the new targeted collection will impair the United States' ability to detect and prevent potential terrorist attacks. When the Government is enjoined from effectuating a statute

enacted by Congress, it almost invariably suffers a form of irreparable injury entitling it to a stay pending appeal. *See opinions cited supra at p.* 4.

The USA FREEDOM Act reflects the judgment of Congress and the President that a targeted collection approach can appropriately serve the United States' interests in national security while further enhancing the substantial protections for personal privacy already built into the Section 215 program. But until that system can come on-line, the statute ensures that the important function of the bulk telephony-metadata program will continue during the transition period. *Clapper*, 2015 WL 6516757, at *6 ("The 180-day transition period represents Congress's considered judgment that there should be time for an orderly transition from the existing program to the new, targeted surveillance program."). The district court's injunction would create the very intelligence gap that Congress sought to avoid. Where the political branches have already reasonably weighed the policy considerations concerning the best way to terminate the Section 215 program and transition to the new targeted collection framework, it was inappropriate for the district court to impose an injunction that requires the abrupt termination of the program. *See Clapper*, 2015 WL 6516757, at *6 (refusing to enter injunction because "[t]he intention of the democratically elected branches of government is thus clear").

Any potential harm of a stay to the Little plaintiffs is minimal. Even assuming these plaintiffs could show that bulk collection of telephony metadata under Section 215 injures them in some way, that program will come to an orderly and planned end

in less than three weeks. Thus, any risk of ongoing injury would be exceedingly modest at most. The Little plaintiffs, moreover, waited over two years – and more than four months into the 180-day transition period – to seek judicial relief, which not only gives rise to a laches bar to their claim but also demonstrates that it is not plausible for them to contend that the program inflicts more than a minimal injury on them. *See* Gov't Prelim. Inj. Opp. (Dkt. # 150) at 24 n. 12.

In any event, plaintiffs have not even demonstrated that the Section 215 program injures them in any way. Pursuant to court orders, NSA analysts may only review records responsive to queries using selectors the Foreign Intelligence Surveillance Court has approved based on reasonable, articulable suspicion that they are associated with identified foreign terrorist organizations. Primary Order, No. 15-99, at 6-7 (*see* Attachment D); Potter Decl. ¶ 23. As a result, only a "tiny fraction" of the records is ever seen by any person. Shea Decl. (Dkt. # 150-2) ¶ 23 (*see* Attachment C). Plaintiffs do not even suggest that the NSA has accessed records of their calls as a result of queries made under the "reasonable, articulable suspicion" standard or otherwise. Thus, there is no basis to conclude that records of plaintiffs' calls have been reviewed (much less that they will be during the remaining three weeks of the Section 215 program), or "used against" plaintiffs in some unexplained way. The district court's conclusion that plaintiffs were entitled to an injunction, therefore, was in error. *See Weinberger* v. *Romero-Barcelo*, 456 U.S. 305, 311-13 (1982).

On balance, therefore, a stay is necessary to protect the government's and the public's strong interest in continuing an important counter-intelligence program to avoid harm to national security during the transition, as Congress has provided. Indeed, even absent Congress's determination, a transition period would have been appropriate to implement an injunction against the program. As the Second Circuit has explained, "[a]llowing the program to remain in place for the short period that remains is the prudent course," and "would likely have been appropriate even had [that court] held § 215 unconstitutional" before Congress enacted the USA FREEDOM Act. *Clapper*, 2015 WL 6516757, at * 9.

B. The Government Has a Strong Likelihood of Success on Appeal.

The government has a strong likelihood of success on appeal, a factor that also favors issuance of a stay. The government need not establish "an absolute certainty of success" to obtain a stay, but rather must demonstrate, at a minimum, "serious legal questions going to the merits." *Population Inst.* v. *McPherson*, 797 F.2d 1062, 1078 (D.C. Cir. 1986).

1. Plaintiffs Lack Standing and Therefore Lack Any Right to Relief.

Standing is an essential element of ultimate success on the merits, without which plaintiffs are not entitled to any relief. To establish standing, plaintiffs must show that they have suffered injury in fact, "an invasion of a legally protected interest," *Lujan* v. *Defenders of Wildlife*, 504 U.S. 555, 560 (1992), that is "concrete, particularized, and actual or imminent." *Clapper* v. *Amnesty Int'l USA*, 133 S. Ct. 1138,

1147 (2013). A "threatened injury must be *certainly impending* to constitute injury in fact," whereas "[a]llegations of *possible* future injury are not sufficient." *Id.*

As explained above, the Little plaintiffs have failed to satisfy that standard because, even assuming, *contra Smith* v. *Maryland*, 442 U.S. 735 (1979), that they have a protected Fourth Amendment privacy interest in metadata relating to their calls, they have not shown that any collection of that metadata under Section 215 has resulted in an actual injury. Given that the bulk collection under Section 215 will continue for less than three weeks, and any queries of the metadata must be court-approved under the "reasonable, articulable suspicion" standard, plaintiffs have failed to show any imminent injury sufficient to establish standing.[2]

2. Bulk Collection of Telephony Metadata Does Not Constitute a Search Within the Meaning of the Fourth Amendment.

Even if plaintiffs could establish standing, the Supreme Court has already rejected plaintiff's underlying Fourth Amendment argument that there is a reasonable expectation of privacy in telephony metadata such that the Section 215 program constitutes a search within the meaning of the Fourth Amendment. In *Smith* v. *Maryland*, the Supreme Court held that the government's recording of the numbers dialed from an individual's home telephone, through the installation of a pen register

[2] In addition, the Little plaintiffs presented no evidence that their provider, Verizon Business Network Services, currently participates in the Section 215 program. The district court improperly speculated that that was true. Slip Op. at 24-25. But such speculation does not rise to the level of certainty required by *Amnesty International* for standing purposes in this context. 133 S. Ct. at 1147.

at a telephone company, is *not* a search under the Fourth Amendment. 442 U.S. 735, 743-44 (1979); *see also United States* v. *Miller*, 425 U.S. 435, 440-45 (1976) (holding that bank customers have no reasonable expectation of privacy in bank records pertaining to them). Except for the district court below, every other court to have decided this constitutional issue – including numerous decisions of the Foreign Intelligence Surveillance Court – has correctly looked to the Supreme Court's holding in *Smith* to conclude that the acquisition from telecommunications companies of business records consisting of bulk telephony metadata is not a search for purposes of the Fourth Amendment.[3]

The grounds on which the district court purported to differentiate the pen-register recording in *Smith* from the Section 215 program – in brief, the duration, breadth, and quantity of data collection – did not factor into the Supreme Court's decision in *Smith*. *See* 442 U.S. at 742-45. Rather, *Smith*'s holding was anchored in the established principle that individuals have no protected expectation of privacy in information they provide to third parties. *Id.* at 743-44. For those reasons, the district court's conclusion that *Smith* is distinguishable is wrong. Indeed, the Second

[3] *See Opinion & Order, In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, No. BR 14-01, 2014 WL 5463097 (FISA Ct. Mar. 20 2014); *Mem. Op., In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, No. BR 14-96, 2014 WL 5463290 (FISA Ct. June 19, 2014); *Smith* v. *Obama*, 2014 WL 2506421, at *4 (D. Idaho June 3, 2014); *ACLU* v. *Clapper*, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013), *rev'd on other grounds*, 785 F.3d 787 (2d Cir. 2015); *United States* v. *Moalin*, 2013 WL 6079518, at *5-8 (S.D. Cal. Nov. 18, 2013); *cf. ACLU* v. *Clapper*, 785 F.3d 787, 821-25 (2d Cir. 2015) (reserving the question).

Circuit found it "difficult to conclude" that litigants such as plaintiffs here are likely to succeed "in arguing that new conditions require a reconsideration of the reach of [such] a long-established precedent" as *Smith*. *Clapper*, 2015 WL 6516757, at *8. Thus, given the conclusive, controlling effect of *Smith*, plaintiffs are not likely to succeed on the merits of their Fourth Amendment claim.

3. Even if Bulk Collection of Telephony Metadata Could Constitute a Fourth Amendment Search, it was Reasonable for Congress to Continue the Program During the Transition Period.

Even if plaintiffs were correct that obtaining bulk telephony metadata from the business records of telecommunications companies constitutes a Fourth Amendment search, it would nevertheless be constitutionally permissible, and especially so to permit continued operation of the Section 215 program for less than three weeks until NSA implements the new statutory system of targeted collection. The Fourth Amendment bars only unreasonable searches and seizures, and continuance of the Section 215 telephony-metadata program for less than three weeks is reasonable under the standard applicable to searches that serve "special needs" of the government. *See, e.g., Vernonia Sch. Dist. 47J* v. *Acton*, 515 U.S. 646, 653 (1995); *Hartness* v. *Bush*, 919 F.2d 170, 173 (D.C. Cir. 1990). The national security and safety interests served by the Section 215 program are special needs of the utmost importance. *See Hartness*, 919 F. 2d at 173; *Cassidy* v. *Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006).

To assess reasonableness under the "special needs" doctrine, courts must "employ[] a balancing test that weigh[s] the intrusion on the individual's [constitutionally protected] interest[s]" against the "'special needs' that support[] the program." *Ferguson* v. *City of Charleston*, 532 U.S. 67, 78 (2001). The purpose of the Section 215 program – identifying unknown terrorist operatives and preventing terrorist attacks – is undisputed and weighty, as even the district court recognized. *Klayman*, 957 F. Supp. 2d at 39; Slip Op. at 37.

The district court, however, refused to acknowledge the important contribution that the Section 215 program makes to the Nation's security, because the government had "still not cited a single instance in which telephone metadata analysis actually stopped an imminent attack." Slip Op. at 35. But that misunderstands the reasonableness inquiry under the special needs doctrine. The precedents of the Supreme Court and this Court (among others) upholding searches as reasonable do not depend on specific instances of success in achieving a particular goal but instead assess whether the program is at least a "reasonably effective means" of advancing the government's paramount interest in preventing terrorism. *Bd. of Educ.* v. *Earls*, 536 U.S. 822, 837 (2002). The Fourth Amendment's reasonableness inquiry does not turn on the identification of specific threats prevented by the program. In any event, the reasonableness of the program and the importance of its aims are further supported by the FBI's views that the capabilities of the Section 215 program remain an important part of its counter-terrorism arsenal, especially in the current, heightened

threat environment. Paarmann Decl. ¶¶ 6-12. The district court improperly gave short shrift to those serious concerns. *See* Slip Op. at 35 n.21.

Balanced against the important purposes served by the Section 215 program during the transition period is the minimal impact the program will have on the Little plaintiffs' privacy interests before it terminates on November 29, 2015.

First, any infringement on plaintiffs' privacy interests attributable to NSA collection of bulk telephony metadata is diminished by its upcoming termination. Indeed, the Second Circuit recently denied a preliminary injunction against the Section 215 program, in part because the plaintiffs' constitutional claims would soon be rendered moot by the program's termination. *Clapper*, 2105 WL 6516757, at *8-9.

Moreover, the district court virtually ignored the restrictions on review and dissemination of the metadata, which have been enhanced since the district court's December 2013 ruling, stating that "there continues to be *no minimization procedures* applicable at the collection stage." Slip Op. at 33. But those restrictions, which require court authorization for any selectors used to conduct queries and limit query result to metadata within two steps of suspected terrorist selectors, greatly diminish the potential for unwarranted intrusions on plaintiffs' privacy interests.

Indeed, now that the USA FREEDOM Act has established a definite end to the Section 215 program, the odds that any metadata pertaining to the Little plaintiffs' calls will be reviewed *in the next three weeks* are miniscule. Similarly, any infringement on plaintiffs' privacy due to the NSA's accumulating another three weeks of bulk data

is substantially mitigated by the fact that, after November 29, 2015, NSA analysts will no longer be permitted to query that data for analytic purposes.

These developments strengthen the government's special-needs argument. The government's interest in preserving its capacity to detect terrorist threats, in the midst of an evolving threat environment, during the brief remainder of the transition until the targeted program of telephony metadata becomes fully operational, far outweighs the now-reduced potential for infringement of plaintiffs' privacy.

CONCLUSION

The district court has enjoined operation of a counter-terrorism intelligence-gathering program authorized by statute and by numerous court orders. For the reasons explained above, this Court should (1) stay the district court order pending appeal or (2) enter an immediate administrative stay until this motion is resolved, and should it be denied, until ten days after such denial so that the government can seek relief from the Supreme Court, if warranted.

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

CHANNING D. PHILLIPS
United States Attorney

DOUGLAS N. LETTER
H. THOMAS BYRON III
(202) 616-5367
CATHERINE H. DORSEY
(202) 514-3469
Attorneys, Appellate Staff
Civil Division, Room 7236
Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

CERTIFICATE OF SERVICE

I hereby certify that on November 10, 2015, I caused the foregoing Emergency Motion for Stay Pending Appeal and for Immediate Administrative Stay to be filed with the Clerk of Court for the United States Court of Appeals for the District of Columbia Circuit by causing an original to be electronically filed via ECF, along with four copies to be hand delivered to the court, and by causing one copy to be served on the following counsel by ECF:

Larry Klayman, Esq.
General Counsel
Freedom Watch, Inc.
D.C. Bar No. 334581
2020 Pennsylvania Avenue NW, Suite 345
Washington, DC 20006
Telephone: (310) 595-0800
Email: leklayman@gmail.com

/s/ Catherine H. Dorsey
CATHERINE H. DORSEY
Catherine.Dorsey@usdoj.gov

Attachment A

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KLAYMAN et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	**Civil Action No. 13-851 (RJL)**
	)	
OBAMA et al.,	)	
	)	
Defendants.	)	

MEMORANDUM OPINION
November 9, 2015 [Dkt. #149]

Our Circuit Court has remanded this case for me to determine whether limited discovery is appropriate to satisfy the standing requirements set forth by the Supreme Court in an earlier national security surveillance case: *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013). Although familiarity with the record and my prior opinion on December 16, 2013[1] is likely, I will briefly recount the history of this matter.

On November 18, 2013, I held a hearing on a motion filed by plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange to preliminarily enjoin the National Security Agency ("NSA") from collecting and querying their telephony metadata pursuant to the NSA's classified bulk telephony metadata collection program (the "Bulk Telephony Metadata Program" or the "Program"), under which the NSA indiscriminately

[1] *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

collects the telephone call records of millions of Americans. Four weeks later, on December 16, 2013, I issued a lengthy opinion ("my December 2013 Opinion") granting the motion as to plaintiffs Larry Klayman and Charles Strange after finding that they had demonstrated a substantial likelihood of success on their Fourth Amendment claim that the collection and querying of their records constituted an unconstitutional search. However, because of the novelty of the legal issues presented and the monumental national security interests at stake, I stayed the injunction pending the appellate review that would undoubtedly follow. Indeed, I assumed that the appeal would proceed expeditiously, especially considering that the USA PATRIOT Act, the statute pursuant to which the NSA was acting, was due to expire on June 1, 2015—a mere eighteen months later. For reasons unknown to me, it did not. Instead, our Circuit Court heard argument on November 4, 2014 and did not issue its decision until August 28, 2015—nearly three months *after* the USA PATRIOT Act had lapsed and had been replaced by the USA FREEDOM Act, which was enacted on June 2, 2015.

As it pertains to this Opinion, the USA FREEDOM Act specifically prohibits the bulk collection of telephony metadata, but not until November 29, 2015. During the intervening 180-day period, the NSA is continuing to operate the Bulk Telephony Metadata Program while it transitions to a new, more targeted program whereby the NSA, pursuant to authorization by the Foreign Intelligence Surveillance Court ("FISC"), can require telecommunications service providers to run targeted queries against their customers' telephony metadata records and then produce the results of those queries to the NSA. Thus, when our Circuit Court issued its decision on August 28, 2015 vacating

my preliminary injunction for a lack of standing and remanding the case to this Court for further proceedings consistent therewith, nearly half of the 180-day transition period had already lapsed.

As a consequence, I immediately scheduled a status conference for the following week to discuss with the parties how to proceed, if at all, prior to the mandate issuing from the Court of Appeals.[2] On August 31, 2015, the Government moved to continue the status conference. I denied that motion. At the status conference on September 2, 2015, Mr. Klayman indicated, among other things, that he intended to seek expedited issuance of the mandate from the Court of Appeals and to amend his complaint by joining new parties who are customers of Verizon Business Network Services ("VBNS") and who therefore, consistent with the Court of Appeals decision, likely had standing to challenge the Program. As expected, on September 8, 2015, plaintiffs sought leave to file a Fourth Amended Complaint that adds plaintiffs J.J. Little and his law firm, J.J. Little & Associates, P.C. ("Little plaintiffs"), both of which are, and at "all material times" were,

[2] Once a case is appealed, a district court lacks jurisdiction over "those aspects of the case involved in the appeal" until the court of appeals issues its mandate. *Griggs v. Provident Consumer Discount Co.*, 459 U.S. 56, 58 (1982) ("The filing of a notice of appeal is an event of jurisdictional significance—it confers jurisdiction on the court of appeals and divests the district court of its control over those aspects of the case involved in the appeal"); *see also United States v. Defries*, 129 F.3d 1293, 1302 (D.C. Cir. 1997) ("The district court does not regain jurisdiction over those issues [that have been appealed] until the court of appeals issues its mandate."). Under the Federal Rules of Appellate Procedure, the mandate will not issue until "7 days after the time to file a petition for rehearing expires, or 7 days after entry of an order denying a timely petition for panel rehearing, petition for rehearing en banc, or motion for stay of mandate, whichever is later." Fed. R. App. P. 41(b). However, the Court of Appeals has "discretion to direct immediate issuance of its mandate in an appropriate case" and parties have "the right . . . at any time to move for expedited issuance of the mandate for good cause shown." D.C. Cir. R. 41(a)(1).

VBNS subscribers. Fourth Am. Compl. ¶ 18 [Dkt. #145-1]. At a September 16, 2015 hearing on this motion, I granted plaintiffs' motion to amend the complaint—which was uncontested—and set a briefing schedule for a renewed motion for preliminary injunction. On September 21, 2015, plaintiffs filed a Renewed Motion for Preliminary Injunction [Dkt. #149], seeking to enjoin as unconstitutional the Bulk Telephony Metadata Program, which is still in operation until November 29, 2015. On October 6, 2015, the Court of Appeals issued its mandate. I heard oral argument on plaintiffs' renewed motion for preliminary injunction two days later.

After careful consideration of the parties' pleadings, the representations made at the October 8, 2015 motion hearing, and the applicable law, I have concluded that limited discovery is not necessary since several of the plaintiffs now are likely to have standing to challenge the constitutionality of the Bulk Metadata Collection Program, and those that do have standing are entitled to preliminary injunctive relief. Accordingly, the Court will GRANT, in part, plaintiffs' Renewed Motion for Preliminary Injunction as it pertains to plaintiffs J.J. Little and J.J. Little & Associates and ENJOIN the future collection and querying of their telephone record metadata.

BACKGROUND

A brief overview of the statutory framework and procedural posture, focusing on developments since my last Opinion in this case, may be a helpful place to start.

A. Statutory Framework

1. The Section 215 Bulk Telephony Metadata Program

Beginning in 1998, the Foreign Intelligence Surveillance Act ("FISA") permitted the FBI to merely apply for an ex parte order authorizing specified entities, such as common carriers, to release to the FBI copies of "business records" upon 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." Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, § 602, 112 Stat. 2396, 2410 (1998). Following the September 11, 2001 terrorist attacks, however, Congress expanded this "business records" provision under Section 215 of the USA PATRIOT Act, to authorize the FBI to apply "for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 501, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861(a)(1)). Thereafter, in March 2006, Congress strengthened the protections in Section 215, amending the statute to provide that the FBI's application must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." USA PATRIOT

Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192, 196 (2006) (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

Although the daily bulk collection, storage, and analysis of telephony metadata is not expressly authorized by the terms of Section 215, beginning in May 2006, the Government, advocating a very aggressive reading of Section 215, sought and received FISC authorization to operate the Bulk Telephony Metadata Program, which, of course, consists of these very practices. *See* Decl. of Acting Assistant Dir. Robert J. Holley, FBI ¶ 6 [Dkt. #25-5] ("Holley Decl."); Decl. of Teresa H. Shea, Signals Intelligence Dir., NSA ¶ 13 [Dkt. # 25-4] ("Shea Decl."); *see also* Decl. of Major General Gregg C. Potter, Signals Intelligence Deputy Dir., NSA ¶ 2 [Dkt. #150-4] ("Potter Decl."). The FISC has repeatedly endorsed this view ever since. Shea Decl. ¶¶ 13-14.[3] As such, for more than seven years, the Government has obtained ex parte orders from the FISC directing telecommunications service providers to produce, on a daily basis, the telephony metadata for each of their subscriber's calls—this includes the dialing and receiving numbers and the date, time, and duration of the calls. It does not, however, include the substantive content of the call. Shea Decl. ¶¶ 7, 13-15, 18; *see* Primary Order, *In re Application of the [FBI] for an Order Requiring the Prod. of Tangible Things From [Redacted]*, No. BR 13-158 at 3 n.1 (FISC Oct. 11, 2013) (attached as Ex. B to Gilligan

[3] Notably, the Second Circuit recently disagreed, holding that, although Section 215 of the USA PATRIOT Act "sweeps broadly," it did not authorize the indiscriminate, daily bulk collection of metadata. *ACLU v. Clapper*, 785 F.3d 787, 821 (2d Cir. 2015) ("For all of the above reasons, we hold that the text of § 215 cannot bear the weight the government asks us to assign to it, and that it does not authorize the telephone metadata program. We do so comfortably in the full understanding that if Congress chooses to authorize such a far-reaching and unprecedented program, it has every opportunity to do so, and to do so unambiguously.").

Decl.) [Dkt. #25-3] ("Oct. 11, 2013 Primary Order"). Once this data is collected from various telecommunications companies, it is consolidated and retained in a single Government database for five years. *See* Shea Decl. ¶¶ 23, 30; *see* Oct. 11, 2013 Primary Order at 14 ¶ E. In this database, the NSA conducts computerized searches that are designed to discern whether certain terrorist organizations are communicating with persons located in the United States. Holley Decl. ¶ 5; Shea Decl. ¶¶ 8-10, 44-63; *see* Am. Mem. Op., *In re Application of the [FBI] for an Order Requiring the Prod. of Tangible Things from [REDACTED]*, No. BR 13-109 at 18-22 (FISC Aug. 29, 2013) (attached as Ex. A to Gilligan Decl.) [Dkt. #25-2]. Despite the Program's broad reach, since a series of leaks exposed the existence of this Program in 2013, the Government has maintained that it "has never captured information on all (or virtually all) calls made and/or received in the U.S." Gov't's Opp'n 5.

Shortly after my December 2013 Opinion, however, President Obama issued an order requiring several important changes to the manner in which these searches are authorized and conducted. *See* President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence; Potter Decl. ¶¶ 5-7. As initially authorized by the FISC, NSA intelligence analysists could conduct searches in the database *without* prior judicial authorization.[4] *See* Shea Decl. ¶ 19. This is no longer

[4] Searches in the database are conducted using "identifiers" such as suspected terrorist telephone numbers—so-called "seeds"— to "chain" or elucidate terrorist communications within the United States. Prior to January 2014, an "identifier" had to be approved by one of twenty-two designated officials in the NSA's Homeland Security Analysis Center or other parts of the

the case. Rather, except in emergency circumstances, NSA analysts are now required to seek approval from the FISC prior to conducting database queries. Potter Decl. ¶ 7. The FISC may only authorize a search if there is a "reasonable, articulable suspicion" ("RAS") that the selection term to be queried (i.e., the "identifier" or "seed") is associated with one or more of the specified foreign terrorist organizations approved for targeting by the FISC. *Id.* Moreover, at the time of my previous Opinion, query results included communication records within "three hops" of the seed identifier. *See* Shea Decl. ¶ 22. Since President Obama's order in January 2014, however, query results have been limited to records of communications within *two* "hops" from the seed, not three. Pottter Decl. ¶ 7. Stated differently, the query results include identifiers and the associated metadata having direct contact with the seed (the first "hop") and identifiers and associated metadata having a direct contact with first "hop" identifiers (the second "hop"). It remains the case that once a query is conducted and it returns a universe of responsive records, NSA analysts may then perform new searches and otherwise perform intelligence analysis *within* that universe of data without using RAS-approved search terms. *See* Shea Decl. ¶ 26.

2. The USA FREEDOM Act

Reacting to significant public outcry regarding the existence of the Bulk Telephony Metadata Program, President Obama called upon Congress to replace the

---

NSA's Signals Intelligence Directorate. Shea Decl. ¶¶ 19, 31. Such approval could be given only upon a determination by one of those designated officials that there exist facts giving rise to a "reasonable, articulable suspicion" ("RAS") that the selection term to be queried is associated with one or more of the specified foreign terrorist organizations approved for targeting by the FISC. *Id.* ¶¶ 20, 31; Holley Decl. ¶¶ 15-16.

Program with one that would "give the public greater confidence that their privacy is appropriately protected," while maintaining the intelligence tools needed "to keep us safe." President Barack Obama, Statement by the President on the Section 215 Bulk Metadata Program (Mar. 27, 2014), http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program. In response to this directive, Congress ultimately enacted the USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015) ("USA FREEDOM Act"), on June 2, 2015. Relevant to this Opinion, the USA FREEDOM Act expressly prohibits the Government from obtaining telephony metadata in bulk, but not until November 29, 2015. USA FREEDOM Act §§ 103, 109; *see* Potter Decl. ¶ 11. It seems that the NSA requested this 180-day delay to allow time to transition from the Bulk Telephony Metadata Program to a new replacement program Congress conceived—a model whereby targeted queries will be carried out against metadata held by telecommunications service providers and the resulting data subsequently produced to the Government. *See id.* § 101. As the Government has explained, this 180-day transition period will avoid a so-called "intelligence gap" that would follow if the current Program terminated before the new targeted metadata querying program is fully operational. Gov't's Opp'n 34; *see* 161 Cong. Rec. S3275 (daily ed. May 22, 2015) (statement of Sen. Leahy) (having printed in the record a letter from the NSA which stated: "NSA assesses that the transition of the program to a query at the provider model is achievable within 180 days, with provider cooperation. . . . [W]e 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."). To date, however, the Government has failed to identify any concrete consequences that would likely result from this so-called "intelligence gap." And while Congress refrained for obvious political reasons from expressly authorizing a six-month extension of the Bulk Telephony Metadata Program,[5] the Government conveniently went immediately thereafter to the FISC to seek judicial authorization to continue the Program during the transition period, consistent with its prior authorization under the USA PATRIOT Act. *See* Mem. of Law 5, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, No. BR 15-75 (FISC June 2, 2015). Not surprisingly, the FISC agreed. *See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, No. BR 15-75 (FISC June 29, 2015). As such, during the current 180-day transition period, the Bulk Telephony Metadata Program has continued by judicial, not legislative, fiat.[6]

B. Procedural Posture

I first had occasion to address plaintiffs' constitutional challenges to the Program in December 2013, when I enjoined the Government from further collecting plaintiffs'

---

[5] The enactment of the USA FREEDOM Act has been described as "signal[ing] a cultural turning point for the nation, almost 14 years after the Sept. 11 attacks heralded the construction of a powerful national security apparatus," which began with significant public backlash to the June 2013 revelation that the NSA was operating a classified bulk metadata collection program. Jennifer Steinhauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 is Sharply Limited*, N.Y. Times, Jun. 3, 2015, at A1.

[6] It is possible that the metadata collected and stored prior to November 29, 2015 will be retained for some period of time after that date to (1) meet any applicable preservation obligations in pending litigation and (2) conduct technical analysis for a three-month period to ensure that the production of call-detail records under the targeted collection program yields similar results to queries of metadata under the retiring Program. Potter Decl. ¶ 15. In any event, the Government represents that analytic access to the data will cease on November 29, 2015. *Id.*

call records under the Program. *Klayman v. Obama*, 957 F. Supp. 2d 1, 44-45 (D.D.C. 2013) (Leon, J.). I concluded, in so ruling, that plaintiffs Klayman and Charles Strange likely had standing to challenge both the bulk collection of metadata under the Program and the ensuing analysis of that data through the NSA's electronic querying process.[7] *Id.* at 26-29. As to the merits of plaintiffs' claims, I found it significantly likely that plaintiffs would be able to prove that the Program violated their reasonable expectation of privacy and therefore was a Fourth Amendment search. *Id.* at 30-37. I held, moreover, that the Program likely failed to meet the Fourth Amendment's reasonableness requirement because the substantial intrusion occasioned by the Program far outweighed any contribution to national security. *Id.* at 37-42. Because the loss of constitutional freedoms is an "irreparable injury" of the highest order, and relief to two of the named plaintiffs would not undermine national security interests, I found that a preliminary injunction was not merely warranted—it was *required*. *Id.* at 42-43. Cognizant, however, of the "significant national security interests at stake," and optimistic that our Circuit Court would expeditiously address plaintiffs' claims, I voluntarily stayed my order pending appeal. *See id.* at 43-44.

As stated previously, our Circuit Court did not do so. Moreover, when it finally issued its decision on August 28, 2015, it did so with considerable brevity. In three separate opinions, the Circuit Court vacated my preliminary injunction on the ground that

[7] Because plaintiffs pled no facts showing that plaintiff Mary Ann Strange was a Verizon Wireless subscriber, let alone a subscriber of any other phone services, I found that she lacked standing to pursue her claims and therefore restricted the remainder of my analysis to the claims advanced by plaintiffs Larry Klayman and Charles Strange. *See Klayman*, 957 F Supp. 2d at 8 & n.5, 43 n.69.

plaintiffs, as subscribers of Verizon Wireless rather than as subscribers of VBNS—the sole provider the Government has acknowledged has participated in the Program—had not shown a substantial likelihood of standing to pursue their claims. *Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015) (per curiam).[8] Left undecided—indeed wholly untouched—was the question of whether a program that indiscriminately collects citizens' telephone metadata constitutes an unconstitutional search under the Fourth Amendment.

Not surprisingly, plaintiffs moved for, and quickly obtained, leave to file a Fourth Amended Complaint. *See* Sept. 16, 2015 Min. Entry. This latest iteration of the Complaint alters plaintiffs' contentions in two material respects. First, it adds plaintiffs J.J. Little and his law firm, J.J. Little & Associates, P.C., both of which are, and at "all material times" were, VBNS subscribers. Fourth Am. Compl. ¶ 18.[9] Second, it sets forth

---

[8] Judge Brown concluded that plaintiffs had demonstrated a *possibility* that their call records are, or were, collected, but because they had not shown a *substantial likelihood* that this was the case, they fell "short of meeting the higher burden of proof required for a preliminary injunction." *Id.* at 562-64. Judge Williams opined that because "[p]laintiffs are subscribers of Verizon Wireless, not of Verizon Business Network Services, Inc.—the sole provider that the government has acknowledged targeting for bulk collection," plaintiffs "lack direct evidence that records involving their calls have actually been collected." *Id.* at 565 (Williams, J.). Given that the Government has neither confirmed nor denied Verizon Wireless's participation in the Program, Judge Williams found plaintiffs' inference that their data was collected too speculative to "demonstrate a 'substantial likelihood' of injury." *Id.* at 566. Judge Sentelle "agree[d] with virtually everything in Judge Williams' opinion," save for his conclusion that the case should be remanded instead of dismissed. *Id.* at 569-70. Like Judge Williams, Judge Sentelle opined that plaintiffs "never in any fashion demonstrate[d] that the [G]overnment is or has been collecting [call-detail] records from their [carrier]" and that the Supreme Court's rejection of similar inferential leaps in *Clapper v. Amnesty International, USA*, 133 S. Ct. 1138 (2013), counsels against finding standing here. *Id.* at 569.

[9] Plaintiffs furnished additional support for this claim in the Supplemental Declaration of J.J. Little, in which he avers that "I and my law firm J.J. Little Associates, P.C. have been customers (subscribers) of Verizon Business Network Services and also Verizon Wireless since October

additional facts intended to bolster plaintiffs' allegation that Verizon Wireless participated in the Program. *Id.* ¶¶ 47-48.

On September 21, 2015, plaintiffs filed a renewed motion for a preliminary injunction, seeking relief, once again, from the "warrantless surveillance" of their telephone calls. *See* Plaintiffs' Renewed Mot. for Prelim. Inj. & Req. for Oral Arg. Thereon [Dkt. #149]. Government defendants, of course, opposed, *see* Government Defendants' Opposition to Plaintiffs' Renewed Motion for a Preliminary Injunction [Dkt. #150] ("Gov't's Opp'n"), and plaintiffs quickly lodged their reply, *see* Plaintiffs' Reply in Support of their Renewed Motion for Preliminary Injunction [Dkt. #152]. On October 6, 2015, our Circuit Court granted plaintiffs' unopposed request for expedited issuance of the mandate, Order, *Obama v. Klayman*, No. 14-5004 (D.C. Cir. Oct. 6, 2015), thereby reinstating this Court's jurisdiction to decide plaintiffs' renewed motion, *see* Mandate [Dkt. #154]. I took plaintiffs' motion under advisement at the conclusion of oral argument on October 8, 2015.

ANALYSIS

I will confine my analysis to the merits of plaintiffs' request for a preliminary injunction and will not address the jurisdictional predicate for my actions, which I discussed at length in my December 2013 Opinion.[10] When ruling on a motion for

---

2011, and have been so continuously during the period from October 2011 until the present." Suppl. Decl. of J.J. Little [Dkt. #152-1].

[10] Specifically, I discussed this Court's jurisdictional authority to review plaintiffs' constitutional claims. *See Klayman*, 957 F. Supp. 2d at 24-25. In sum, I found that Congress had not stated with the requisite clarity any intent to preclude judicial review of constitutional claims related to FISC orders by any non-FISC courts. *See Webster v. Doe*, 486 U.S. 592, 603 (1988) ("[W]here

preliminary injunction, a court must consider "whether (1) the plaintiff has a substantial likelihood of success on the merits; (2) the plaintiff would suffer irreparable injury were an injunction not granted; (3) an injunction would substantially injure other interested parties; and (4) the grant of an injunction would further the public interest." *Sottera, Inc. v. Food & Drug Admin.*, 627 F.3d 891, 893 (D.C. Cir. 2010) (internal quotation marks omitted).[11] I will address each of these factors in turn.

A. Plaintiffs Have Shown a Substantial Likelihood of Success on the Merits.

My analysis of plaintiffs' likelihood of success on the merits of their constitutional claims focuses exclusively on their Fourth Amendment challenges, which I find most likely to succeed.[12] I begin, however, as I did previously, with plaintiffs' standing to

---

Congress intends to preclude judicial review of constitutional claims its intent to do so must be clear."); *see also Elgin v. Dep't of the Treasury*, 132 S. Ct. 2126, 2132 (2012) ("[A] necessary predicate to the application of *Webster*'s heightened standard [is] a statute that purports to deny any judicial forum for a colorable constitutional claim." (internal quotation marks omitted)); *McBryde v. Comm. to Review Circuit Council Conduct & Disability Orders of the Judicial Conference of the U.S.*, 264 F.3d 52, 59 (D.C. Cir. 2001) (finding "preclusion of review for both as applied and facial constitutional challenges only if the evidence of congressional intent to preclude is 'clear and convincing'").

[11] Our Circuit has traditionally applied a "sliding scale" approach to these four factors. *Davis v. Pension Benefit Guar. Corp.*, 571 F.3d 1288, 1291-92 (D.C. Cir. 2009). In other words, "a strong showing on one factor could make up for a weaker showing on another." *Sherley v. Sebelius*, 644 F.3d 388, 392 (D.C. Cir. 2011). Following the Supreme Court's decision in *Winter v. NRDC, Inc.*, 555 U.S. 7 (2008), however, our Circuit suggested, without deciding, that "*Winter* could be read to create a more demanding burden." *Davis*, 571 F.3d at 1292. Thus, while it is unclear whether the "sliding scale" remains controlling in light of *Winter*, the Court need not decide that issue today because I conclude that plaintiffs have carried their burden of persuasion as to all four factors.

[12] The Second Circuit recently declined to issue a preliminary injunction in a similar case, holding that the USA FREEDOM Act authorized the 180-day continuation of the Bulk Telephony Metadata Program and declining to reach the "momentous constitutional issues" raised by the limited continuation of the Program. *ACLU v. Clapper*, No. 14-42-cv (2d Cir. Oct. 29, 2015). In refusing to consider the constitutional questions raised, the Second Circuit noted that it "ought not meddle with Congress's considered decision" to continue the Program for a

challenge the Bulk Telephony Metadata Program. *See Jack's Canoes & Kayaks, LLC v. Nat'l Park Serv.*, 933 F. Supp. 2d 58, 76 (D.D.C. 2013) ("The first component of the likelihood of success on the merits prong usually examines whether the plaintiffs have standing in a given case." (internal quotation marks omitted)).

1. Plaintiffs are Substantially Likely to Have Standing to Challenge the Bulk Telephony Metadata Program.

Plaintiffs Larry Klayman, Charles Strange, Mary Ann Strange, J.J. Little, and J.J. Little & Associates, P.C. challenge the past and future collection of their telephone metadata, as well as the analysis of that data through the NSA's electronic querying process. After careful consideration of these challenges, I conclude that while plaintiffs J.J. Little and J.J. Little & Associates, P.C. have standing to proceed, plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange do not.

No principle is more fundamental to the balance of federal power 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 omitted). Inherent in this principle is the requirement that each plaintiff demonstrate adequate standing to press their claims in federal court. *Raines v. Byrd*, 521 U.S. 811, 818 (1997). "To establish Article III standing, an injury must be 'concrete,

---

limited transition period and that doing so would not be a "prudent use of judicial authority" given that rendering a decision on such difficult constitutional questions would almost certainly take longer than the time remaining for the Program's operation. *Id.* at 23. Fortunately for this Court, my analysis of these "momentous constitutional issues" began nearly two years ago, and so I do not suffer the same time constraints. Moreover, as I explain below, this Court cannot, and will not, sit idle in the face of likely constitutional violations for fear that it might be viewed as meddling with the decision of a legislative branch that lacked the political will, or votes, to *expressly* and unambiguously authorize the Program for another six months.

particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Clapper v. Amnesty Int'l USA* ("*Clapper*"), 133 S. Ct. 1138, 1147 (2013) (quoting *Monsanto Co. v. Geerston Seed Farms*, 561 U.S. 139, 149 (2010)); *see also Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 & n.1 (1992) ("By particularized, we mean that the injury must affect the plaintiff in a personal and individual way."). When the challenged harm is prospective, courts face the additional hurdle of assuring themselves that its likelihood is not too far flung, lest imminence, "a somewhat elastic concept . . . be stretched beyond its purpose" to create a controversy where none exists. *Lujan*, 504 U.S. at 564 n.2. Consequently, the "threatened injury must be *certainly impending*" to prevent litigation of illusory claims. *See Clapper*, 133 S. Ct. at 1147 (internal quotation marks omitted).

Any discussion of standing to challenge a classified Government surveillance program must begin with the seminal case on this issue: *Clapper v. Amnesty International*. *Clapper* concerned a challenge by Amnesty International to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881a, which authorizes the Government to surveil non-United States persons reasonably believed to be located outside the United States. 133 S. Ct. at 1142. There, plaintiffs, "United States persons whose work . . . requires them to engage in sensitive international communications with individuals who they believe are likely targets of surveillance under § 1881a," sought declaratory and injunctive relief from surveillance under the statute. *Id.* The issue before the Supreme Court was whether plaintiffs had standing to seek prospective relief. They did not. According to the Supreme Court, plaintiffs' claims

failed because their allegations rested on a series of contingencies that may—or may not—come to pass. Specifically, success required: that plaintiffs' foreign contacts would be targeted for surveillance under the challenged statute; that the FISC would approve the surveillance; that the government would *actually* intercept communications from plaintiffs' foreign contacts; and that plaintiffs' communications would be among those captured. *Id.* at 1148. Without reaching the merits of plaintiffs' claims, the Supreme Court held that plaintiffs had not established standing because their "theory of *future* injury [was] too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'" *Id.* at 1143 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). Whether *Clapper's* use of the term "certainly impending" imposes a higher threshold for standing, or merely adds gloss to the longstanding requirement of "concreteness," is unclear.[13] What *Clapper* does instruct, however, is that standing to challenge a classified Government surveillance program demands more than speculation that the challenged surveillance has, or will, transpire.

[13] As the *Clapper* majority pointed out in a footnote, "[o]ur cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur." *Clapper*, 133 S. Ct. at 1150 n.5. The Court declined, however, to comment further because it found plaintiffs' allegations too "attenuated" to demonstrate harm. Indeed, Justice Breyer, in his dissent, expressed doubt as to whether there is a meaningful difference between a "substantial risk" of future harm and a risk of "clearly impending harm." *Id.* at 1160-61 (Breyer, J., dissenting). In his view, "the case law uses the word 'certainly' as if it emphasizes, rather than literally defines, the immediately following term 'impending.'" *Id.* at 1161 (Breyer, J., dissenting). That is to say, whether "substantial risk" and "clearly impending" impose substantively different standing requirements, or lexical variations of the same overarching standard, is a question for another day. In any event, I need not reach this issue because I find that the Little plaintiffs have met the threshold for "certainly impending" injury.

On appeal here, our Circuit Court found that plaintiffs Klayman and Charles Strange's alleged injuries were too attenuated to constitute "concrete and particularized injury" as required by *Clapper*. *See Klayman*, 800 F.3d at 562 (Brown, J.) (internal quotation marks omitted). According to all three of our Circuit Judges, because plaintiffs had adduced no proof that "*their own* metadata was collected by the government" under the Program, they had not demonstrated a substantial likelihood of standing to pursue their claims. *Id.* at 562-63 (Brown, J.); *see also id.* at 565 (Williams, J.) ("[P]laintiffs lack direct evidence that records involving their calls have actually been collected."); *id.* at 569 (Sentelle, J., dissenting in part) ("[P]laintiffs never in any fashion demonstrate that the government is or has been collecting such records from their telecommunications provider."). Fortunately for plaintiffs, our Circuit's holding did not sound the death knell for their cause.

On September 16, 2015, plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange filed an uncontested Fourth Amended Complaint, joining as plaintiffs to the action VBNS subscribers J.J. Little and J.J. Little & Associates. *See* Fourth Am. Compl. Separately, and in an attempt to bolster their standing as Verizon Wireless subscribers, plaintiffs appended to their Complaint a document they claim shows that Verizon Wireless was "at all material times" participating in the Program. *See* Fourth Am. Compl. ¶ 47. I will begin by addressing plaintiffs' renewed arguments that Verizon Wireless was, and continues to be, a participant in the Program before turning to the merits of plaintiffs' alternative argument that the Little plaintiffs have standing to proceed.

Unfortunately for plaintiffs Klayman and Strange, I must conclude, in light of our Circuit's ruling in this case, that they have not adequately substantiated their injuries on remand. Plaintiffs appended to the Complaint a de-classified letter from the Department of Justice to the then-Presiding Judge of the FISC, Judge John D. Bates, regarding a "Compliance Incident Involving In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from . . . Cellco Partnership d/b/a Verizon Wireless." *See* Fourth Am. Compl. Ex. 1 [Dkt. #145-1]. Plaintiffs apparently interpret this document as confirmation that Verizon Wireless participated in the Program. Fourth Am. Compl. ¶¶ 47-48. The Government contends that it does no such thing. Gov't's Opp'n 17-18. While plaintiffs' suspicion is plausible, if not logical,[14] based on our Circuit Court's reasoning, I must agree with the Government that this document does not prove Verizon Wireless was ordered to turn over the metadata records of its customers. In fact, a Verizon spokesman suggested that the use of "Verizon Wireless" may simply be a vestige of "the government's practice to use broad language covering all of Verizon's entities in headings of such court orders . . . regardless of whether any specific part was required to provide information under that order." *See* Charlie Savage, *N.S.A. Used Phone Records Program to Seek Iran Operatives*, N.Y. Times, Aug. 12, 2015 (attached as Ex. 2 to Fourth Am. Compl.). As such, plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange have not shown a substantial likelihood that their telephony metadata

[14] Indeed, I went to great lengths in my December 2013 Opinion to debunk the notion that the NSA had omitted from the Program the single largest wireless carrier in the United States and in so doing had collected a universe of metadata so woefully incomplete as to undermine the Program's putative purpose. *See Klayman*, 957 F. Supp. 2d at 27. In my judgment, common sense still dictates that very conclusion regarding Verizon Wireless' participation in the Program.

was collected pursuant to the Program and therefore are not entitled to a preliminary injunction.

Quite the opposite, however, is true for the Little plaintiffs. The "irreducible constitutional minimum of standing" requires that plaintiffs "must have suffered an 'injury in fact'—an invasion of a legally protected interest which is . . . concrete and particularized." *Lujan*, 504 U.S. at 560. According to our Circuit Court, this demands evidence that "the [P]rogram targets plaintiffs." *See Klayman*, 800 F.3d at 567 (Williams, J.); *see also id.* at 563 (Brown, J.) (declining to find standing because "the facts marshaled by plaintiffs do not fully establish that their own metadata was ever collected"). The Little plaintiffs emphatically meet this hurdle. They aver in their Fourth Amended Complaint that "Little, for himself and by and through his law firm, J.J. Little & Associates, has been and continues to be a subscriber of Verizon Business Network Services for his firm J.J. Little & Associates, P.C." Fourth Am. Compl. ¶ 18. Their subscription has, moreover, been "continuous[]" since October 2011. Suppl. Decl. of J.J. Little ¶ 2 [Dkt. #152-1].[15] Because the Government has acknowledged that VBNS subscribers' call records were collected during a three-month window in which the Little plaintiffs were themselves VBNS subscribers, barring some unimaginable circumstances, it is overwhelmingly likely that their telephone metadata was indeed warehoused by the NSA. The Little plaintiffs, then, have pled facts wholly unlike those in *Clapper*. There is

[15] Indeed, as the Government defendants note in their brief, a district court found standing in a nearly identical set of circumstances in which the plaintiff "submitted specific testimonial evidence that it had received telephone service from VBNS 'since 2007' and continued to do so at the time it moved for injunctive relief. Gov't's Opp'n 19 n.9 (citing *ACLU v. Clapper*, No. 1:13-cv-3994 (S.D.N.Y.)).

no need to speculate that their metadata was targeted for collection, that the challenged Program was used to effectuate the metadata collection, that the FISC approved these actions, or that VBNS subscriber call records were indeed collected. Simply stated, *Clapper*'s "'speculative chain of possibilities' is, in this context, a reality." *ACLU v. Clapper*, 785 F.3d 787, 802 (2d Cir. 2015).

Given the strong presumption that the NSA collected, and warehoused, the Little plaintiffs' data within the past five years, these plaintiffs unquestionably have standing to enjoin any future queries of that metadata. The Government protests that there is "no evidence that the NSA has accessed records of [plaintiffs'] calls as a result of queries made under the 'reasonable, articulable suspicion' standard or otherwise." Gov't's Opp'n 20. To them, it is pure "conjecture" that "records of Plaintiffs' calls have been" or "will be" reviewed "during the remaining two months of the Section 215 program." Gov't's Opp'n 20. I wholeheartedly disagree. As I explained in my December 2013 Opinion, every single time the NSA runs a query to, for example, "detect foreign identifiers associated with a foreign terrorist organization calling into the U.S.," it must "analyze metadata for *every* phone number in the database by comparing the foreign target number against *all* of the stored call records to determine which U.S. phones, if any, have interacted with the target number." *Klayman*, 957 F. Supp. 2d at 28 (internal quotation marks omitted). The Second Circuit, not surprisingly, completely agrees. There, a court tasked with a substantially similar inquiry opined that the NSA "necessarily searches [plaintiffs'] records electronically, even if such a search does not

return [their] records for close review by a human agent." *See ACLU*, 785 F.3d at 802.[16] As the Second Circuit also points out, computerized searches "might lessen the intrusion," but they do not obviate it altogether. *Id.* A search remains a search regardless of how it is effectuated. If the Program is unlawful—and for the reasons discussed herein I believe it is substantially likely that it is—plaintiffs have suffered a concrete harm traceable to the challenged Program and redressable by a favorable ruling. For that reason, I find that the Little plaintiffs have "standing to object to the collection and review of their data."[17] *See id.*

Whether the Little plaintiffs have standing to challenge the *future* collection of their telephone metadata requires a separate analysis. The Government contends that the Little plaintiffs lack such standing because "there is no evidence before the Court that VBNS is currently a participating provider in the [Program]." Gov't's Opp'n 19. To them, "[a]n assumption that the NSA 'must be' collecting bulk telephony metadata from VBNS today because it did so for a three-month period in 2013 is precisely the sort of inference that the D.C. Circuit held in *Klayman* falls short of the certainty required under

---

[16] The analogy I used in my December 2013 Opinion remains instructive. Suppose one enters a hypothetical library to find each and every book citing *Battle Cry of Freedom* as a source. Suppose further that this goal has judicial pre-approval. *Battle Cry of Freedom* "might be referenced in a thousand books. It might be in just ten. It could be in zero. The only way to know is to check every book. At the end of a very long month, you are left with the 'hop one' results (those books that cite *Battle Cry of Freedom*), but to get there, you had to open every book in the library." *Klayman*, 957 F. Supp. 2d at 28 n.38.

[17] Brief mention must be made of the Government's argument that even if their data was collected, warehouse, and queried, the Little plaintiffs have failed to show a redressable injury. Specifically, the Government claims that plaintiffs lack standing because they have no "legally protected interest" in the collection and review of their telephone metadata. *See* Gov't's Opp'n 22. I held in my December 2013 Opinion that plaintiffs were likely to prove that the NSA's retrieval and querying process is indeed a Fourth Amendment search and decline to revisit that decision here. *See Klayman*, 957 F. Supp. 2d at 37.

[*Clapper*] to establish a plaintiff's standing in a case of this nature." Gov't's Opp'n 19. The Government's argument misconstrues what is required to establish standing in a case such as this. As I indicated *supra*, *Clapper* does not render Article III the enemy of every challenge to a classified surveillance program. Standing, in a post-*Clapper* world, remains an obstacle for the quixotic litigant, but is not a roadblock for the truly aggrieved. Rather, *Clapper* must be understood as it was unequivocally written: to stymie attenuated claims of harm. In that respect, our Circuit's holding in *Klayman* clearly abides. *See Klayman*, 800 F.3d at 566 (Brown, J.) (noting that Amnesty International's challenge in *Clapper* failed because plaintiffs "had no actual knowledge of the Government's § 1881a targeting practices nor could they even show that the surveillance program they were challenging even existed" (internal quotation marks omitted)); *see also id.* at 567 (Williams, J.) (likening plaintiffs' "assertion that NSA's collection must be comprehensive in order for the program to be effective" to the *Clapper* plaintiffs' speculative "assertions regarding the government's motive and capacity to target their communications"). According to our Circuit, a "substantial likelihood" of standing cannot rest on inferences about *which providers* participated in *this particular* Program. This proposition, however, does not mean that courts must abandon all common sense in determining the *scope* of that participation once concretely pled. Indeed, nothing in our Circuit Court's opinion precludes me from inferring, based on the NSA's past collection of VBNS subscriber data, that it continues to collect bulk telephony metadata from that *same* provider, pursuant to the *same* statutory authorization, to combat the *same* potential threats to our national security.

Indeed, common sense leads to that precise conclusion here. To start, I need not speculate that the Government continues to operate this Program. It has acknowledged as much. Potter Decl. ¶ 14. Proof that the Government *has* collected VBNS subscribers' metadata is, moreover, persuasive evidence that the threat of *ongoing* collection is not "chimerical." *See Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2345 (2014) (quoting *Steffel v. Thompson*, 415 U.S. 415, 459 (1973)). While the Government has not admitted that it continues to collect VBNS subscriber call records, its avowed need to combat terrorism makes it overwhelmingly likely that it does. According to Bryan Paarmann, Deputy Assistant Director of the Counterterrorism Division in the National Security Branch of the FBI, "[t]he threat environment confronting the United States has evolved" since this Court last opined. Paarmann Decl. ¶ 5 [Dkt. #150-6]. "Over the past two years the United States has confronted, and is still confronting, an increasing threat of attacks by individuals who act in relative isolation or in small groups." *Id.* This "increasingly diffuse threat environment" demands, under the FBI's logic, increased vigilance. *See* Paarmann Decl. ¶ 9; *see also id.* ¶ 11 ("[T]he current terrorist threat environment underscores the significance of this key ["contact chaining"] capability under the bulk telephony metadata program.").

The Government's position that VBNS may no longer be a participant in the Program is fundamentally at odds with its ever-escalating concerns of terrorist threats. By the Government's own admission, it is marshaling all available investigative tools to combat a threat it believes to be least as menacing as it was in 2013. *See* Paarmann Decl. ¶ 9. It defies common sense for defendants to argue, as they apparently do, that the

Government has chosen to omit from this breathtakingly broad metadata collection Program a provider that the Government surveilled in the past and that, presumably, has the infrastructure to continue assisting in that surveillance. In fact, it would make no sense whatsoever for the Government to use all available tools *except* VBNS call data to accomplish its putative goals. I am not alone in reaching this conclusion. The Second Circuit itself recently held that VBNS subscribers have standing to bring nearly identical claims because evidence that plaintiffs' "call records are indeed among those collected," made it unnecessary to speculate that the government "may in the future collect[] their call records." *ACLU*, 785 F.3d at 801. This is an imminent harm that is, once again, traceable to the challenged statute and remediable by a prospective injunction. Therefore, I find that the Little plaintiffs have standing to seek an order enjoining the future collection of their telephone metadata because they have shown a substantial likelihood that the NSA has collected and analyzed their telephone metadata and will continue to do so consistent with FISC opinions and orders. At the present time, no further amount of discovery is necessary to resolve the standing issue. Whether the Government's actions violate plaintiffs' Fourth Amendment rights is, of course, the province of the next section.

2. Plaintiffs are Likely to Succeed on the Merits of Their Fourth Amendment Claim.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. That right "shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the

place to be searched, and the persons or things to be seized." *Id.* A Fourth Amendment "search" occurs when "the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). In my December 2013 Opinion, I explained at length why both the indiscriminate bulk collection of telephony metadata and the analysis of that data each separately constitute a search within the meaning of the Fourth Amendment. *Klayman*, 957 F. Supp. 2d at 30-37. Neither the recent changes in the operation of the Program, nor the passage of the USA FREEDOM Act, has done anything to alter this analysis. The fact remains that the indiscriminate, daily bulk collection, long-term retention, and analysis of telephony metadata almost certainly violates a person's reasonable expectation of privacy.

Therefore, whether plaintiffs are entitled to preliminary injunctive relief at this stage turns on whether those searches are likely to be unreasonable, in light of intervening changes in the law. *See Kyllo*, 533 U.S. at 31 (whether a search has occurred is an "antecedent question" to whether a search was reasonable). Notwithstanding the Government's strong protestations, I conclude that plaintiffs will likely succeed in showing that the searches during this 180-day transition period still fail to pass constitutional muster.

a. Plaintiffs Will Likely Prove that the Searches Are Unreasonable.

The Fourth Amendment prohibits unreasonable searches. *See Samson v. California*, 547 U.S. 843, 848 (2006). Whether a search is reasonable depends on the totality of the circumstances. *Id.* Typically, searches not conducted pursuant to a warrant

based on the requisite showing of probable cause are "*per se* unreasonable." *Nat'l Fed'n of Fed. Emps.-IAM v. Vilsack*, 681 F.3d 483, 488-89 (D.C. Cir. 2012) (quoting *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010)). The Supreme Court, however, has recognized limited exceptions to this rule, including for situations in which "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (internal quotation marks omitted). Evaluating whether a warrantless, suspicionless search is reasonable under the "special needs" doctrine requires a court to balance the privacy interests implicated by the search against the governmental interest furthered by the intrusion. *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665-66 (1989).[18] Specifically, I must balance: (1) "the nature of the privacy interest allegedly compromised" by the search, (2) "the character of the intrusion imposed" by the

[18] Several categories of searches have been upheld under the "special needs" doctrine. Schools are permitted under certain circumstances to test students for drugs. *See Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls*, 536 U.S. 822, 838 (2002) (upholding urinalysis for all public school students participating in extracurricular activities); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 656 (1995) (upholding urinalysis for public school student athletes). The same is true for searches conducted by certain government employers. *See Von Raab*, 489 U.S. at 679 (upholding drug testing of Customs Service employees who applied for promotion to positions involving interdiction of illegal drugs or which required them to carry a firearm); *Willner v. Thornburgh*, 928 F.2d 1185, 1193-94 (D.C. Cir. 1991) (upholding urine tests of applicants for positions as attorneys at the Department of Justice). Officers may search probationers and parolees to ensure compliance with the rules of supervision. *See Griffin*, 483 U.S. at 880. And, in some cases, law enforcement may conduct suspicionless searches to prevent acts of terrorism in transportation centers. *See Cassidy v. Chertoff*, 471 F.3d 67, 87 (2d Cir. 2006) (upholding suspicionless searches of carry-on baggage and automobile trunks on Lake Champlain ferries); *MacWade v. Kelly*, 460 F.3d 260, 275 (2d Cir. 2006) (upholding searches of bags in New York City subway system). Suspicionless seizures have also been upheld under similar balancing analysis, including highway checkpoints designed to detect illegal entrants into the Unites States, *United States v. Martinez-Fuerte*, 428 U.S. 543, 567 (1976), and to catch intoxicated motorists, *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 455 (1990).

Government, and (3) "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them." *See Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls*, 536 U.S. 822, 830-34 (2002).

In my December 2013 Opinion, I held that the NSA's Bulk Telephony Metadata Program likely violated the Fourth Amendment because "plaintiffs [had] a substantial likelihood of showing that their privacy interests outweigh[ed] the Government's interest in collecting and analyzing bulk telephony metadata." *Klayman*, 957 F. Supp. 2d at 41. In opposition to plaintiffs' renewed motion for preliminary injunction, the Government argues that several developments since December 2013 have altered the special needs analysis such that plaintiffs are no longer likely to prevail. Gov't's Opp'n 33. For the following reasons, I do not agree.

i. Nature of the Privacy Interest

My analysis of the reasonableness of the searches at issue in this case begins with the nature of the privacy interest at stake. As I explained at length in my December 2013 Opinion, plaintiffs have a very significant expectation of privacy in an aggregated collection of their telephony metadata. *See Klayman*, 957 F. Supp. 2d at 32-37. When a person's metadata is aggregated over time, in this case five years, it can be analyzed to reveal "embedded patterns and relationships, including personal details, habits, and behaviors." Decl. of Prof. Edward W. Felten ¶¶ 24, 38-58 [Dkt. #22-1]. Recognizing that certain factors may diminish a person's otherwise robust privacy expectations, *see Willner v. Thornburgh*, 928 F.2d 1185, 1188 (D.C. Cir. 1991) ("[E]ven a current employee's 'expectation of privacy,' while 'reasonable' enough to make urine testing a

Fourth Amendment 'search,' can be so 'diminished' that the search is not 'unreasonable.'"), I consider this intrusion in the context of Americans' evolving interactions with mobile technology. Indeed, as of this year, 92 percent of American adults own a cellphone, 67 percent of whom own a so-called "smartphone" that enables them to, among other things, connect to the Internet. Lee Rainie & Kathryn Zickuhr, *Americans' Views on Mobile Etiquette*, *Chapter 1: Always on Connectivity*, Pew Research Center (Aug. 26, 2015), http://www.pewinternet.org/2015/08/26/chapter-1-always-on-connectivity/#fn-14328-1. Those who own such phones "often treat them like body appendages," as nine-in-ten cellphone owners carry their phones with them "frequently." *Id.* Smartphones, moreover, are not used merely for their basic communications functions, but rather "to help [owners] navigate numerous important life events," including for the sensitive purposes of online banking and researching health conditions. Aaron Smith, *U.S. Smartphone Use in 2015*, Pew Research Center (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/. The Government is quite right that these facets of mobile technology are not targeted by metadata collection. Nevertheless, Americans' constant use of cellphones for increasingly diverse and private purposes illustrates the attitude with which people approach this technology as a whole. Surely a person's expectation of privacy is not radically different when using his or her cellphone to make a call versus to check his or her bank account balance.

Furthermore, the attitude with which cellphone users approach their devices presents a dramatically different context than the contexts in which courts have upheld

"special needs" searches. Specifically, cellular phone technology does not present the same diminished expectation of privacy that typically characterizes "special needs" incursions. Take, for example, airports. In the context of air travel, courts have recognized that "society has long accepted a heightened level of security and privacy intrusion with regard to air travel." *Cassidy v. Chertoff*, 471 F.3d 67, 76 (2d Cir. 2006). Notably, Americans know that airports are discrete areas in which certain rights otherwise enjoyed are forfeited. *See id.* It is their choice to enter that space and, in so doing, to check certain rights at the door. Not so with cellphones. As already described, cellphones have become a constant presence in people's lives. While plaintiffs' privacy interests in their aggregated metadata may be somewhat diminished by the fact that it is held by third-party service providers, this is a *necessary* reality if one is to use a cellphone at all, and it is, therefore, simply not analogous to the context of voluntarily entering an airport. In this case, plaintiffs have asserted that the NSA's searches were a substantial intrusion on their privacy, and I have no reason to doubt that, nor to find that their privacy expectations should have been diminished given the context. Rather, I conclude that plaintiffs' privacy interests are robust.

ii. Character and Degree of Governmental Intrusion

Turning next to the character and degree of the Government's intrusion on plaintiffs' privacy interest, the Government avers that "[a]t this stage, the [P]rogram's potential for intrusion on Plaintiffs' privacy interests is minimal, and finite." Gov't's Opp'n 37. The Government first notes that the Program will no longer continue indefinitely but will end on November 29, 2015; therefore, any infringement is

necessarily limited in duration. *Id.* The Government next emphasizes that the new restrictions on queries—including that FISC authorization is now required before a query is conducted and that query results are now limited to "two hops"—significantly diminish the likelihood that plaintiffs' data will actually be reviewed. *Id.* Although I agree with the Second Circuit that there is now "a lesser intrusion on [plaintiffs'] privacy than they faced at the time this litigation began," *ACLU*, 785 F.3d at 826, I simply cannot agree with the Government's characterization of it as "minimal, and finite."

When considering whether a search is minimally or substantially intrusive, courts evaluate a variety of factors, including, *inter alia*, "the duration of the search or stop, the manner in which government agents determine which individual to search, the notice given to individuals that they are subject to search and the opportunity to avoid the search . . . as well as the methods employed in the search." *Cassidy*, 471 F.3d at 78-79 (citations omitted); *see also Willner*, 928 F.2d at 1189-90 (discussing as mitigating factors whether the person had "notice of an impending intrusion" and had a "large measure of control over whether he or she will be subject to" the search).

To say the least, the searches in this case lack most of these hallmarks of minimal intrusion. It is not, as an initial matter, a discrete or targeted incursion. To the contrary, it is a sweeping, and truly astounding program that targets millions of Americans arbitrarily and indiscriminately. To be sure, by designing a program that eliminates the need for agents to use discretion, the Government has reduced to zero the likelihood that metadata will be collected in a discriminatory fashion—a characteristic that the Supreme Court has suggested minimizes the privacy intrusion. *See, e.g.*, *United States v.*

Martinez-Fuerte, 428 U.S. 543, 559 (1976) (noting that roving patrols presented "a grave danger [of] unreviewable discretion," while fixed checkpoints reduce the scope of the intrusion because it "regularize[s]" enforcement). It is, however, absurd to suggest that the Constitution favors, or even tolerates, such extreme measures! To this Court's knowledge, no program has ever been upheld under the "special needs" doctrine that was not tailored, even if imperfectly, in some meaningful way.[19] Yet in this case the Government has made *no* attempt to tailor its program at all. *See Earls*, 536 U.S. at 852 (Ginsburg, J., dissenting) ("There is a difference between imperfect tailoring and no tailoring at all.").

Furthermore, although the intrusion plaintiffs now face may be "finite" in duration, it is certainly not "short." It is telling indeed that the searches and seizures upheld under the "special needs" doctrine have generally involved searches of significantly limited duration. *See, e.g.*, *Martinez-Fuerte*, 428 U.S. at 546-47 (upholding warrantless stops at a vehicle checkpoint where the average length of the stop was three

---

[19] Although not yet called upon to review an indiscriminate search of the breadth presented here, the Supreme Court has repeatedly hinted that it would be skeptical of a program that lacked sufficient tailoring. *See Earls*, 536 U.S. at 844 (Ginsburg, J., dissenting) ("Those risks [of illegal drug use], however, are present for *all* schoolchildren. *Vernonia* cannot be read to endorse invasive and suspicionless drug testing of all students upon any evidence of drug use, solely because drugs jeopardize the life and health of those who use them."); *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000) ("[T]he Fourth Amendment would almost certainly permit *an appropriately tailored roadblock* set up to thwart an imminent terrorist attack. The exigencies created by these scenarios are far removed from the circumstances under which authorities might simply stop cars as a matter of course to see if there just happens to be a felon leaving the jurisdiction.") (emphasis added); *see also Cassidy*, 471 F.3d at 80-81 (recognizing the "legitimate concern" that the government's power to conduct suspicionless searches may be limitless given the threat of terrorism is "omnipresent" but finding that concern not implicated "where the government has imposed security requirements only on the nation's largest ferries after making extensive findings about the risk these vessels present in relation to terrorism and . . . the scope of the searches is rather limited").

to five minutes). In contrast, under this Program, the NSA collects data on a *daily basis* and maintains the metadata gathered from those daily searches for *five years*. Moreover, though the weeks remaining in the Program may seem relatively short given that the previous timeframe was *indefinite*, this reduced period still significantly dwarfs the duration of the intrusion in all "special needs" cases of which this Court is aware. With respect to the institution of new procedures for authorizing database queries and the new limitations on the extent of the records returned for review, while these new methods of searching may further mitigate the privacy intrusion that occurs when the NSA queries and analyzes metadata, there continues to be *no minimization procedures* applicable at the collection stage. *See* Oct. 11, 2013 Primary Order at 3-4 (requiring the Order's recipients to turn over all of their metadata without limit).

Finally, far from Americans being put on notice of the Bulk Telephony Metadata Program such that they could choose to avoid it, the Program was, and continues to be, shrouded in secrecy. This may, of course, be practically necessary for the Program to be effective, but it nevertheless increases the level of the privacy intrusion. *See, e.g.*, *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 657 (1995) (analogizing students who choose to participate in athletics to "adults who choose to participate in closely regulated industry"); *Von Raab*, 489 U.S. at 675 n.3 ("When the risk is the jeopardy to hundreds of human lives . . . that danger *alone* meets the test of reasonableness, so long as the search is conducted . . . with reasonable scope and the passenger has been given advance notice of his liability to such a search so that he can avoid it by choosing not to travel by air.") (internal quotation marks omitted); see *also Willner*, 928 F.2d at 1190 ("[T]he applicant's

knowledge of what will be required, and when, affects the strength of his or her interest."). In sum, despite changes to the Program, the Government is still, in effect, asking this Court to sanction a dragnet of unparalleled proportions.

iii. Nature of Government's Interest and Efficacy

Having found that the first two factors militate in plaintiffs' favor, I must finally consider whether the nature of the Government's interest and the efficacy of the Program in meeting its goals are, nevertheless, substantial enough to tip the balance in the Government's favor. As I stated in my December 2013 Opinion, I agree with the Government that the purpose of "identifying unknown terrorist operatives and preventing terrorist attacks" is an interest of the highest order that goes beyond regular law enforcement needs. *Klayman*, 957 F. Supp. 2d at 39 (internal quotation marks omitted). More specifically, though, I found that the Government's true interest was in identifying and investigating imminent threats *faster* than would be otherwise possible.[20] *Id.* at 39-40. Given that the Program's end is only several weeks away, the Government now also argues that the transition period meets the particular need of avoiding the creation of "an intelligence gap in the midst of the continuing terrorist threat." Gov't's Opp'n 34. While an "intelligence gap"—however amorphous its contours—could be significant in theory, the Government has not sufficiently defined it to date to warrant that characterization.

[20] This emphasis remains today, especially in light of the evolving nature of the terrorist threat. *See* Paarmann Decl. ¶ 9 ("Because of this increasingly diffuse threat environment, the availability of all investigative tools that permit the [Government] to detect and respond to terrorist threats quickly, has become increasingly important."); *see also* Gov't's Opp'n 35 ("Analysis of telephony metadata to *quickly* detect contacts of known or suspected terrorists is an important component of the Government's counter-terrorism arsenal.").

But even if it had, proffering a significant special need is not the end of this Court's inquiry. *See City of Indianapolis v. Edmond*, 531 U.S. 32, 42 (2000) ("[T]he gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose."). Rather, I must also evaluate the efficacy of the searches at issue in meeting this need. *See Cassidy*, 471 F.3d at 85-86. To date, the Government has still not cited a single instance in which telephone metadata analysis actually stopped an imminent attack, or otherwise aided the Government in achieving any time-sensitive objective.[21] Although the Government is not required to adduce a specific threat in order to demonstrate that a "special need" exists, *see Earls*, 536 U.S. at 835-36, providing this Court with examples of the Program's success would certainly strengthen the Government's argument regarding the Program's efficacy. This is especially true given that the Program is not designed for detection *and deterrence* like most other programs upheld under the "special needs" doctrine. Indeed, most warrantless searches upheld under the "special needs" doctrine boast *deterrence* as a substantial Governmental interest. For example, screening passengers' bags before allowing them to board a ferry may rarely detect an actual attempt to board with

[21] In the Government's most recent declaration regarding the need for the Program, it states that given "an increasing threat of attacks by individuals who act in relative isolation or in small groups," Paarmann Decl. ¶ 5, including at the encouragement of the Islamic State of Iraq and the Levant and al-Qaeda, "the availability of all investigative tools that permit the FBI and its partners to detect and respond to terrorist threats quickly, has become increasingly important," *id.* at ¶ 9. With respect to the Bulk Telephony Metadata Program, the Government states: "Information gleaned from NSA analysis of telephony metadata *can be* an important component of the information the FBI relies on to identify and disrupt threats," *id.* at ¶ 10 (emphasis added), it "*can provide* information earlier than other investigative methods and techniques," and "earlier receipt of this information *may advance* an investigation and contribute to the disruption of a terrorist attack that, absent the metadata tip, the FBI might not have prevented in time," *id.* at ¶ 12 (emphasis added). Not exactly confidence inspiring!

dangerous substances or devices, but may nevertheless be deemed reasonable because of its deterrent effect. *See Cassidy*, 471 F.3d at 85-86; *see also Von Raab*, 489 U.S. at 675 n.3 ("Nor would we think, *in view of the obvious deterrent purpose of these searches*, that the validity of the Government's airport screening program necessarily turns on whether significant numbers of putative air pirates are actually discovered by the searches." (emphasis added)). The same cannot be said of this Program. Because secrecy is the hallmark of the Program, the deterrent value is effectively zero and its efficacy can only be measured by its ability to detect, and thereby prevent, terrorist attacks.

Nevertheless, instead of providing this Court with specific examples of the Program's success, the Government makes the bootstrap argument that the enactment of the USA FREEDOM Act confirms the importance of this Program to meeting the Government's special needs, Gov't's Opp'n 34, and suggests that this Court should defer to that judgment, *see id.* at 35 n.24. Please! I recognize that my duty to evaluate the efficacy of this Program is "not meant to transfer from politically accountable officials to the courts the decision as to which among reasonable alternative law enforcement techniques should be employed to deal with a serious public danger." *See Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 453 (1990). Nonetheless, while "the choice among such reasonable alternatives remains with the governmental officials," *id.* at 453-54, I must still determine whether the Program is reasonably effective in accomplishing its goals, even if not optimally so, *see Cassidy*, 471 F.3d at 85-86 (noting that a court's task is not to determine whether a particular program is "optimally effective, but whether it [is] reasonably so"). This is a conclusion I simply cannot reach given the continuing lack

of evidence that the Program has ever actually been successful as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism. Accordingly, having determined that the Government has proffered a "special need," but done nothing to abate my lingering doubts about whether the Bulk Telephony Metadata Program is reasonably effective at meeting this need, I find this factor weighs in the Government's favor, but only to a limited extent.

In conclusion, I find that plaintiffs are substantially likely to demonstrate that they have a robust privacy interest in their aggregated metadata and that the intrusion thereon by the Bulk Telephony Metadata Program is substantial. Against these factors, which weigh heavily in plaintiffs' favor, I further find that, although the Government has proffered a compelling "special need" of quickly identifying and investigating potential terror threats, plaintiffs will likely be able to show that the Program is not reasonably effective at meeting this need. Therefore, plaintiffs will likely succeed in showing that the Program is indeed an unreasonable search under the Fourth Amendment.

B. Plaintiffs Will Suffer Irreparable Harm Absent Injunctive Relief.

As I have discussed at length, plaintiffs have demonstrated that they are substantially likely to succeed on their claim that the Government is actively violating the rights guaranteed to them by the Fourth Amendment. Because "[i]t has long been established that the loss of constitutional freedoms, 'for even minimal periods of time, unquestionably constitutes irreparable injury,'" *Mills v. District of Columbia*, 571 F.3d 1304, 1312 (D.C. Cir. 2009) (quoting *Elrod v. Burns*, 427 U.S. 347, 373 (1976)), the

Little plaintiffs have adequately demonstrated irreparable injury. As such, it makes no difference that this violation now has a foreseeable end.[22]

C. The Public Interest and Potential Injury to Other Interested Parties Both Weigh in Plaintiffs' Favor.

The final factors I must consider in weighing plaintiffs' entitlement to preliminary injunctive relief are the balance of the equities and the public interest. *See Sottera*, 627 F.3d at 893. As an initial matter, I emphasize the obvious: "enforcement of an unconstitutional law is always contrary to the public interest." *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013); *see also Hobby Lobby Stores, Inc. v. Sebelius*, 723 F.3d 1114, 1145 (10th Cir. 2013) ("[I]t is always in the public interest to prevent the violation of a party's constitutional rights." (internal quotation marks omitted)), *aff'd sub nom. Burwell v. Hobby Lobby Stores, Inc.*, 134 S. Ct. 2751 (2014); *Melendres v. Arpaio*, 695 F.3d 990, 1002 (9th Cir. 2012) (same); *Am. Freedom Def. Initiative v. Wash. Metro. Area Transit Auth.*, 898 F. Supp. 2d 73, 84 (D.D.C. 2012) (same); *Nat'l Fed'n of Fed. Emps. v. Carlucci*, 680 F. Supp. 416, 435 (D.D.C. 1988) ("[T]he public interest lies

---

[22] Against this presumption, the Government incredibly argues that the Little plaintiffs' claim of irreparable harm is necessarily undercut by their more than two-year delay in joining this suit. Gov't's Opp'n 24 n.12. Come on! While delay in filing may suggest the proffered harm is not truly irreparable, late filing alone is not a sufficient basis for denying a preliminary injunction. *See Gordon v. Holder*, 632 F.3d 722, 724 (D.C. Cir. 2011) ("[A] delay in filing is not a proper basis for denial of a preliminary injunction."). In this case, I do not find the two-year delay to be significant. Although the Government emphasizes the "personal" nature of Fourth Amendment rights, *see* Gov't's Opp'n 29, it was certainly reasonable for the Little plaintiffs to perceive that their rights would ultimately be vindicated by other similarly-situated plaintiffs—the expectation of privacy in their telephony metadata is identical and the searches thereof were reasonably inferred to be the same. *Cf. Cooper v. Aaron*, 78 S. Ct. 1401 (1958) (holding that Arkansas state officials were bound by the Supreme Court's prior decision that racial segregation in public schools was unconstitutional in a case involving four different states that employed a similar system). Until our Circuit Court's decision regarding standing, there was little reason for the Little plaintiffs to believe they were uniquely positioned to challenge the Program.

in enjoining unconstitutional searches."). Given my finding that plaintiffs are likely to succeed on the merits of their Fourth Amendment claim, the public interest weighs heavily in their favor.

Undaunted, the Government argues that the public interest actually counsels *against* granting a preliminary injunction in this case because of the public's strong interest in maintaining an ability to *quickly* identify and investigate terrorist threats. *See* Gov't's Opp'n 45. Indeed, the Government goes one step further by arguing that *United States v. Oakland Cannabis Buyers' Cooperative*, 532 U.S. 483 (2001), requires this Court to defer to Congress's "determination" that continuing the Program during the 180-day transition period is the best way to protect the public's interest.[23] *See* Gov't's Opp'n 38. Not quite! Congress did not *explicitly* authorize a continuation of the Program. Rather, it artfully crafted a starting date for the prohibition of the Program that would enable the Government to confidentially seek FISC authorization to continue the Program for the 180-day transition period and free the Members of Congress from having to vote for an *explicit* extension of the Program. *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 109, 128 Stat. 268, 276 (2015). Moreover, while *Oakland* "prohibits a district court from second-guessing Congress's lawful prioritization of its policy goals," it in no way limits a court from evaluating "the lawfulness of Congress's means of achieving those priorities." *Gordon*, 721 F.3d at 652-53; *see also Vilsack*, 681 F.3d at 490 (noting

[23] In *Oakland*, the district court enjoined the defendant cooperative from distributing marijuana except in cases of medical necessity. In overturning the appeals court decision affirming this injunction, the Supreme Court found that the district court could not ignore Congress's determination, as expressed through legislation, that marijuana has no medical benefits warranting its limited distribution. *Oakland*, 532 U.S. at 496-99.

that "[d]eference is never blind" and "the constitutional question is distinct from policy questions involving otherwise constitutional administrative judgments about how best to operate a program"). Congress, of course, is *not* permitted to prioritize any policy goal over the Constitution. *Gordon*, 721 F.3d at 653. Nor am I! *See Marbury v. Madison*, 5 U.S. 137, 180 (1803) ("Thus, the particular phraseology of the constitution of the United States confirms and strengthens the principle, supposed to be essential to all written constitutions, that a law repugnant to the constitution is void; and that *courts,* as well as other departments, are bound by that instrument.").[24] This Court simply cannot, and will not, allow the Government to trump the Constitution merely because it suits the exigencies of the moment.

This Court's vigilance in upholding the Constitution against encroachment is, of course, especially strong in the context of the Fourth Amendment. Indeed, the Judiciary has long recognized that:

> Moved by whatever momentary evil has aroused their fears, officials—perhaps even supported by a majority of citizens—may be tempted to conduct searches that sacrifice the liberty of each citizen to assuage the perceived evil. But the Fourth Amendment rests on the principle that a true balance between the individual and society depends on the recognition of "the

[24] For this reason, it is unsurprising that the Government has not proffered a single case in which a plaintiff who was likely to prevail on the merits of a constitutional claim was denied a preliminary injunction because of the gravity of the public interest. In *In re Navy Chaplaincy*, 697 F.3d 1171 (D.C. Cir. 2012), our Circuit was reviewing the denial of a preliminary injunction where the District court concluded that although plaintiffs had shown irreparable harm, they were *not* likely to succeed on the merits of their First Amendment claims and the public interest and balance of the equities weighed against them. *Id.* at 1178-79. Similarly, in *Davis v. Billington*, 76 F. Supp. 3d 59 (D.D.C. 2014), the District court denied a request for preliminary injunction where all the preliminary injunction factors weighed against plaintiff, including his likelihood of success on the merits of his constitutional claim. *Id.* at 68-69.

> right to be let alone—the most comprehensive of rights and the right most valued by civilized men."

New Jersey v. T.L.O., 469 U.S. 325, 361-62 (1985) (quoting *Olmstead v. United States,* 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)). To be sure, the very purpose of the Fourth Amendment would be undermined were this Court to defer to Congress's determination that individual liberty should be sacrificed to better combat today's evil.

The Government concludes by discussing at length the negative impact an injunction in this case would have on the Program as a whole, including that the *immediate* cessation of collection of or analytic access to metadata associated with plaintiffs' telephone numbers, if ordered, would require the NSA to terminate the Program altogether. Gov't's Opp'n 41-45. This would be the case, the Government argues, for several reasons. First, the NSA would need to obtain information regarding plaintiffs' telephone numbers and would need to be granted FISC authorization to access the database for the purpose of complying with this Court's order. Gov't's Opp'n 41-42. Beyond these preliminary steps, it would take an undetermined amount of time to develop the technical means to comply with the Court's order, including figuring out how to ensure no new metadata relating to plaintiffs' records is added to the database and how to discontinue analytic access to any metadata relating to plaintiffs' records that is currently in the database. Gov't's Opp'n 43-44. Unfortunately for the Government, this Court does not have much sympathy for these last minute arguments. The Government was given unequivocal notice that it may be required to undertake steps of this nature in my December 2013 Opinion granting plaintiffs' request for a preliminary injunction.

Indeed, I expressly warned against any future request for delay stating, "I fully expect that during the appellate process, which will consume at least the next six months, the Government will take whatever steps necessary to prepare itself to comply with this order when, and if, it is upheld." *Klayman*, 957 F. Supp. 2d at 44. Given that I significantly under-estimated the duration of the appellate process, the Government has now had *over twenty-two months* to develop the technology necessary to comply with this Court's order. To say the least, it is difficult to give meaningful weight to a risk of harm created, in significant part, by the Government's own recalcitrance.

CONCLUSION

With the Government's authority to operate the Bulk Telephony Metadata Program quickly coming to an end, this case is perhaps the last chapter in the Judiciary's evaluation of this particular Program's compatibility with the Constitution. It will not, however, be the last chapter in the ongoing struggle to balance privacy rights and national security interests under our Constitution in an age of evolving technological wizardry. Although this Court appreciates the zealousness with which the Government seeks to protect the citizens of our Nation, that same Government bears just as great a responsibility to protect the individual liberties of those very citizens.

Thus, for all the reasons stated herein, I will grant plaintiffs J.J. Little and J.J. Little & Associates' requests for an injunction[25] and enter an order consistent with this Opinion that (1) bars the Government from collecting, as part of the NSA's Bulk

[25] For reasons stated at the outset, this relief is limited to these plaintiffs. I will deny the motion as it relates to plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange.

Telephony Metadata Program, any telephony metadata associated with these plaintiffs' Verizon Business Network Services accounts and (2) requires the Government to segregate any such metadata in its possession that has already been collected.[26] In my December 2013 Opinion, I stayed my order pending appeal in light of the national security interests at stake and the novelty of the constitutional issues raised. I did so with the optimistic hope that the appeals process would move expeditiously. However, because it has been almost two years since I first found that the NSA's Bulk Telephony Metadata Program likely violates the Constitution and because the loss of constitutional freedoms for even one day is a significant harm, *see Mills*, 571 F.3d at 1312, I will not do so today.

RICHARD J. LEON
United States District Judge

[26] Although it is true that granting plaintiffs the relief they request will force the Government to identify plaintiffs' phone numbers and metadata records, and then subject them to otherwise unnecessary individual scrutiny, *see* Gov't's Opp'n 41-42, that is the only way to remedy the constitutional violations that plaintiffs are substantially likely to prove on the merits.

Attachment B

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KLAYMAN et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	**Civil Action No. 13-0851 (RJL)**
	)	
OBAMA et al.,	)	
	)	
Defendants.	)	

ORDER
(November 9, 2015)

For the reasons set forth in the Memorandum Opinion entered this date, it is hereby

ORDERED that plaintiffs' Renewed Motion for Preliminary Injunction [Dkt. #149] is **GRANTED** as to plaintiffs J.J. Little and J.J. Little & Associates, P.C. and **DENIED** as to plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange; it is further

ORDERED that the Government:

(1) is barred from collecting, as part of the NSA's Bulk Telephony Metadata Program, any telephony metadata associated with J.J. Little and J.J. Little & Associates, P.C. Verizon Business Network Services telephone subscriptions; and

(2) must segregate out all such metadata already collected from any future searches of its metadata database.

SO ORDERED.

RICHARD J. LEON
United States District Judge

Attachment C

EXHIBIT 2

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)]

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.

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

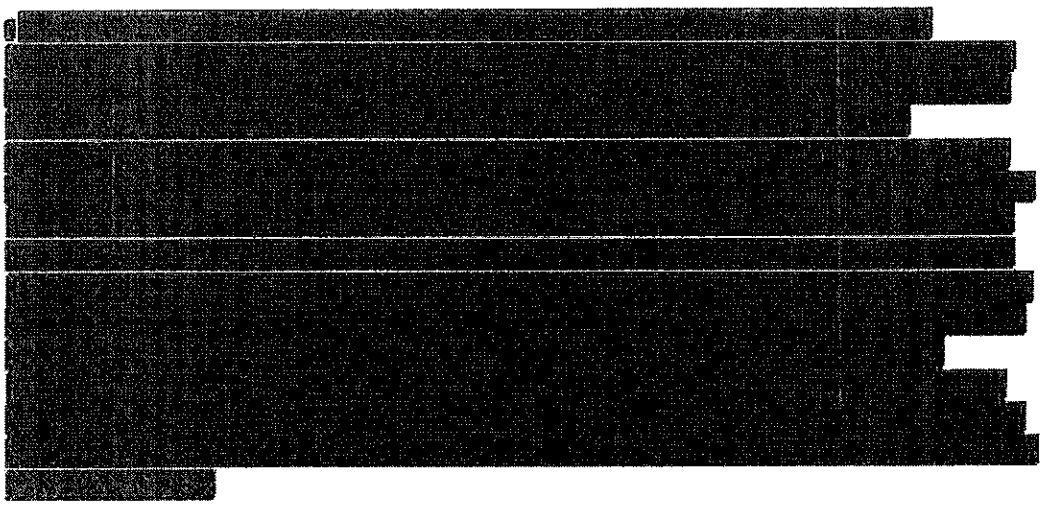
[2] The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA shall ensure that any access

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.



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]

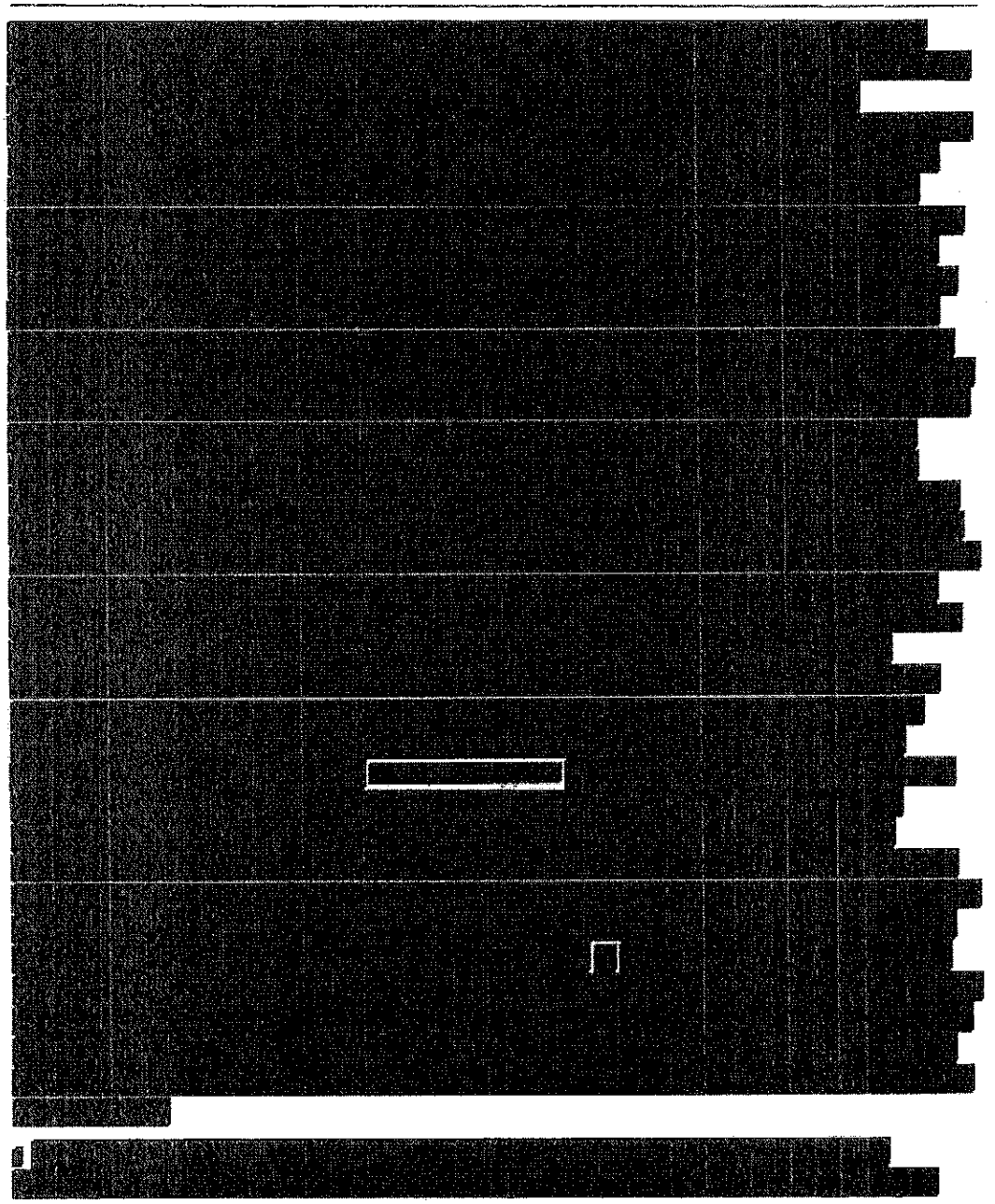
(i) Except as provided in subparagraph (ii) below, all selection terms to be used as "seeds" with which to query the BR metadata shall be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized 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)



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]

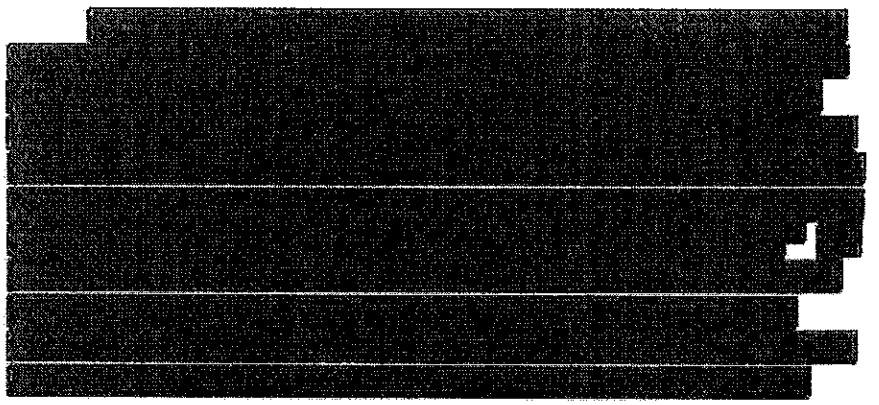
pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(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.

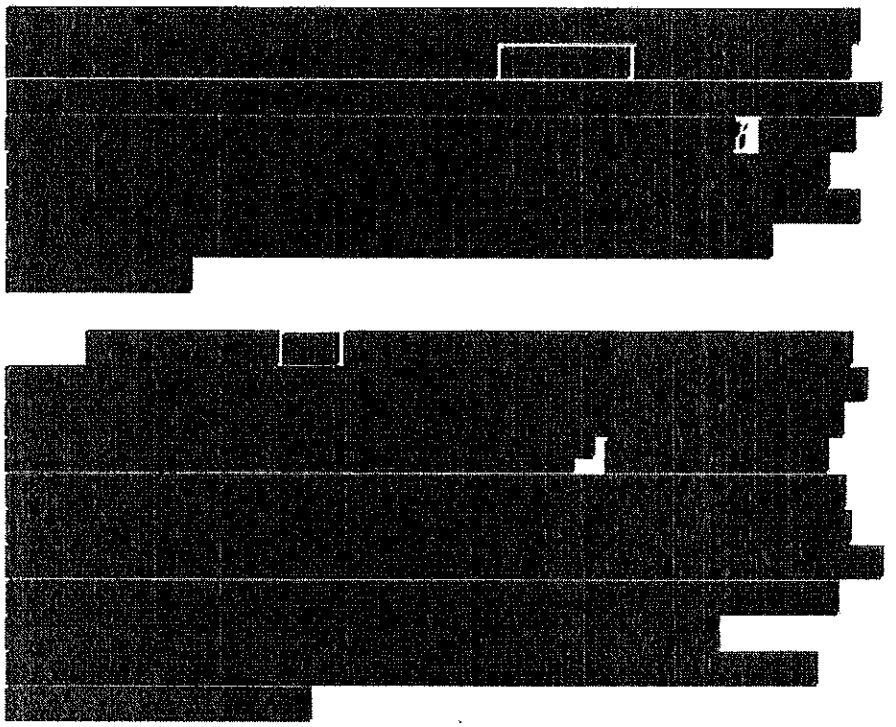
[redacted]

(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:

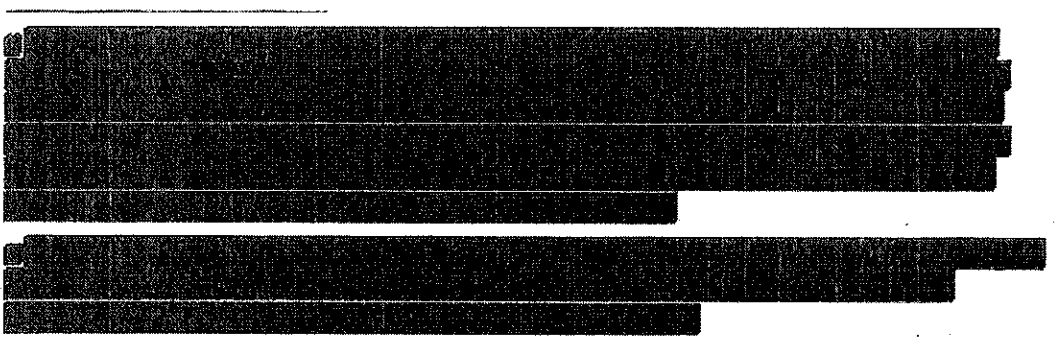


[11] This automated query process was initially approved by this Court in its [redacted] 2012 Order amending docket number [redacted]

[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.



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.[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) 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

[redacted]

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

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)

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

Attachment D

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]

[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.

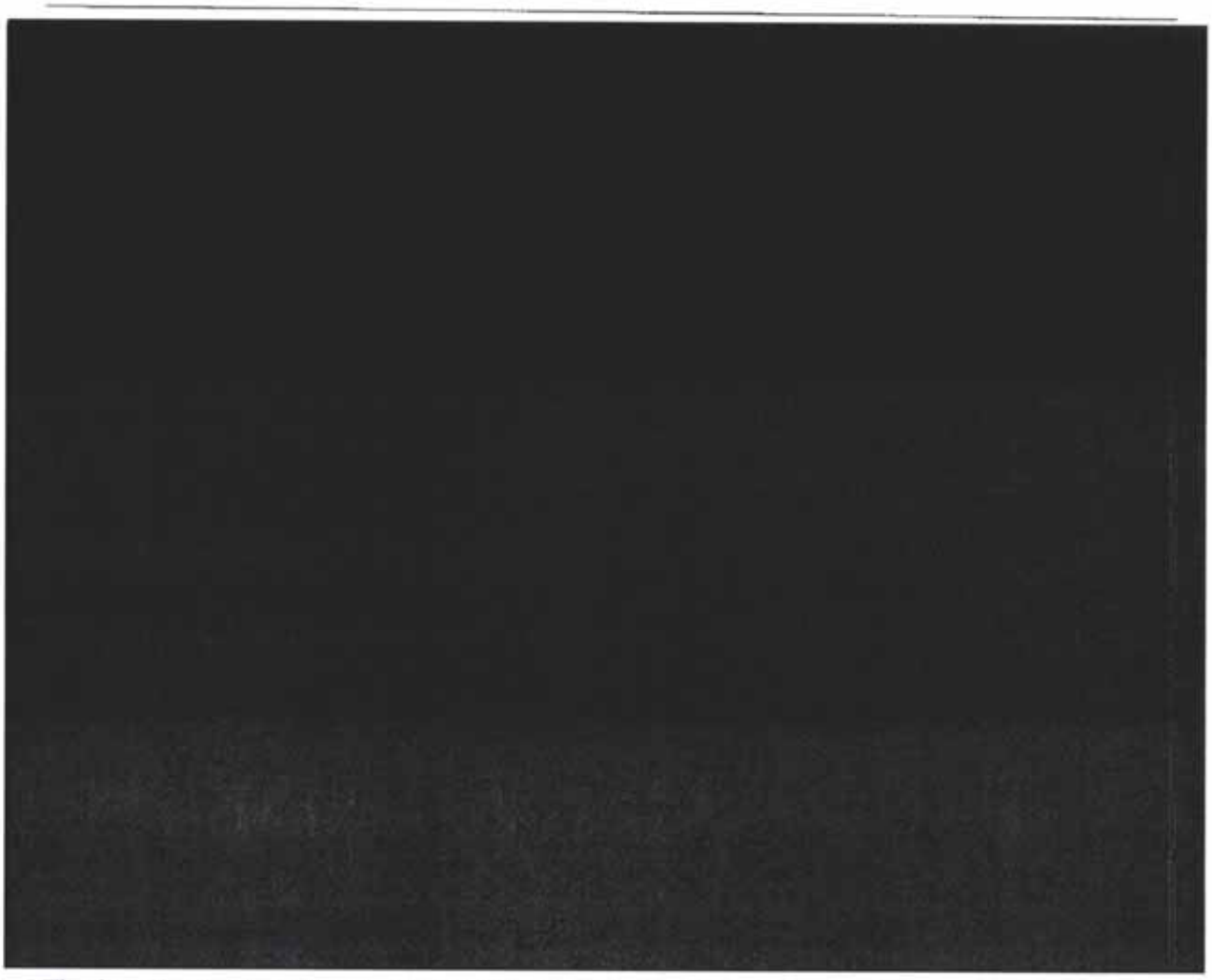
reasonable articulable suspicion (RAS) standard[6] as "seeds" to query the BR metadata for purposes of obtaining foreign intelligence information. The Government may query

---

[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:[illegible]pm 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

Attachment E

EXHIBIT 6

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 C. BRYAN PAARMANN
DEPUTY ASSISTANT DIRECTOR
COUNTERTERRORISM DIVISION
NATIONAL SECURITY BRANCH
FEDERAL BUREAU OF INVESTIGATION

I, C. Bryan Paarmann, state and declare as follows:

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

2. The FBI submits this declaration in the above-captioned case in support of the Government's opposition to the Plaintiffs' renewed motion for a preliminary injunction. I base the statements I make in this declaration upon my personal knowledge and information I have obtained in the course of carrying out my duties and responsibilities as Deputy Assistant Director. I discuss herein the bulk telephony metadata program, authorized by the Foreign Intelligence Surveillance Court (FISC) pursuant to Section 215 of the USA PATRIOT Act, under which the

National Security Agency (NSA) obtains and queries bulk telephony metadata for counterterrorism purposes. Although the existence of the program has been publicly acknowledged by the Government, numerous details about its scope and operation remain classified, and cannot be discussed in a public declaration. I therefore limit my discussion herein to facts about the program that are unclassified in nature.

3. I understand that the USA FREEDOM Act will, as of November 29, 2015, prohibit the Government from collecting bulk telephony metadata as previously authorized by orders issued by the FISC. Under this new legislation, Congress replaced bulk telephony-metadata collection under FISC orders with a new mechanism providing for the targeted production of call-detail records and other tangible things. Congress also provided for a 6-month transition period by delaying for 180 days[1] the effective date of the new prohibition on bulk collection and for the corresponding implementation date of the new regime of targeted production.

4. The purpose of this declaration is to discuss, in unclassified terms, the importance of continuing the bulk telephony metadata program during the transition period in light of the current threat environment, that is to say, the current threat of terrorist attack on the United States, its people, and its interests.

5. Since Plaintiffs first moved for a preliminary injunction in October 2013, the threat environment confronting the United States has evolved. Over the past two years the United States has confronted, and is still confronting, an increasing threat of attacks by individuals who act in relative isolation or in small groups.

[1] Because the USA FREEDOM Act was signed into law on June 2, 2015, the 180 day transition period expires on November 29, 2015.

6. In particular, the Islamic State of Iraq and the Levant ("ISIL") has called for small-scale attacks on the United States, its people, and its interests abroad. Recently, in January 2015, for example, ISIL released a video via social media networking sites reiterating the group's support for lone offender and other small-scale attacks in Western countries. The video specifically advocates for attacks against soldiers, law enforcement, and intelligence community members. Similarly, al-Qaida and its affiliates, such as al-Qaida in the Arabia Peninsula ("AQAP"), have also promoted conducting attacks using simple and inexpensive methods, via its online English language magazine *Inspire*.

7. In contrast to planning large-scale attacks such as the terrorist attacks on the United States on September 11, 2001, which can require months or even years of coordination among dozens of co-conspirators, planning small-scale attacks involves fewer actors and thus can be coordinated and carried out more quickly. The limited number of participants and the swiftness with which the necessary planning can occur may leave fewer clues for investigators who are attempting to prevent or disrupt them. Small-scale terror attacks that have occurred over the last twelve months in the United States, Canada, Europe, and Australia demonstrate that this threat is real.

8. In addition to the increased calls for small scale attacks, increased political instability in some parts of the Middle East over the past two years, including in Syria, has made it more difficult to identify those individuals who seek to attack the United States or our allies before they strike.

9. Because of this increasingly diffuse threat environment, the availability of all investigative tools that permit the FBI and its partners to detect and respond to terrorist threats quickly, has become increasingly important. Indeed, in conjunction with its domestic and

foreign partners, the FBI has been rigorously collecting and analyzing information as it pertains to the ongoing threat posed by ISIL, AQAP, and other foreign terrorist organizations. To do so, the FBI has been using all available investigative techniques and methods to combat the threat these groups may pose to the United States.

10. Although the FBI 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 and most timely analysis occurs when intelligence information obtained from each of those sources can be considered together to compile as complete a picture as possible of a potential terrorist threat. Information gleaned from NSA analysis of telephony metadata can be an important component of the information the FBI relies on to identify and disrupt threats.

11. Telephony metadata can be an important source of timely intelligence in a counterterrorism investigation because analysis of the data permits the Government to determine quickly whether known or suspected terrorist operatives have been in contact with other persons who may be engaged in terrorist activities, including persons and activities within the United States. While the FBI has relied upon such "contact chaining" as a method of detecting foreign espionage networks and operatives for decades, the current terrorist threat environment underscores the significance of this key capability under the bulk telephony metadata program.

12. The sooner we obtain information about particular threats to the national security, the more likely we will be able to prevent and protect against them. Telephony metadata analysis can provide information earlier than other investigative methods and techniques, and can act as an "early warning system" of potential threats against the Nation's security. Especially in the current threat environment, with increased risk of small-scale attacks, earlier

receipt of this information may advance an investigation and contribute to the disruption of a terrorist attack that, absent the metadata tip, the FBI might not have prevented in time.

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

Executed this 1st day of October, 2015.

C. BRYAN PAARMANN
Deputy Assistant Director
Counterterrorism Division
Federal Bureau of Investigation
Washington, D.C.

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

Larry Elliott Klayman, et al., Plaintiffs-Appellees, v. Barack Hussein Obama, et al., Defendants-Appellants.	No. 15-5307

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

A. Parties and Amici

Plaintiffs-appellees are Larry Elliot Klayman, Charles Strange, Mary Ann Strange, J.J. Little, and J.J. Little & Associates, P.C. Defendants-appellants are Barack Obama, President of the United States, Loretta E. Lynch, Attorney General of the United States, and Admiral Michael S. Rogers, Director of the National Security Agency ("NSA"), insofar as they are sued in their official capacities, together with defendants NSA and the

United States Department of Justice (collectively, the government defendants)

B. Ruling Under Review

The ruling under review is Judge Richard J. Leon's order (docket entry # 159) issued November 9, 2015, granting preliminary injunctive relief against the government defendants in district court case No. 13-851 (RJL). The district court also entered on the same day a memorandum opinion (docket entry # 158) accompanying that order.

C. Related Cases

This case has previously been before this Court on the government defendants' appeal of an earlier preliminary injunction in Nos. 14-5004, 14-5016, 14-5005, and 14-5017. This Court reversed and remanded the earlier injunction in a decision issued on August 28, 2015, and reported at 800 F.3d 559.

Respectfully submitted,

DOUGLAS N. LETTER

H. THOMAS BYRON III

(202) 616-5367

CATHERINE H. DORSEY

(202) 514-3469

/s/ Catherine H. Dorsey

Catherine H. Dorsey
(202) 514-3469
Attorneys, Appellate Staff
Civil Division
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Room 7236
Washington, D.C. 20530

NOVEMBER 2015

CERTIFICATE OF SERVICE

I hereby certify that on November 10, 2015, I electronically filed the foregoing with the Clerk of the Court by using the appellate CM/ECF system.

I certify that the participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

/s/ Catherine H. Dorsey
Catherine H. Dorsey

United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 15-5307 **September Term, 2015**

1:13-cv-00851-RJL

Filed On: November 10, 2015

Larry Elliott Klayman, et al.,

Appellees

v.

Barack Obama, et al.,

Appellants

Roger Vinson,

Appellee

National Security Agency and United States Department of Justice,

Appellants

BEFORE: Tatel, Griffith, and Millett, Circuit Judges

O R D E R

Upon consideration of the emergency motion for a stay and for an administrative stay, it is

ORDERED that the district court's order issued November 9, 2015, be stayed pending further order of the court. The purpose of this administrative stay is to give the court sufficient opportunity to consider the merits of the motion for a stay and should not be construed in any way as a ruling on the merits of that motion. See D.C. Circuit Handbook of Practice and Internal Procedures 33 (2015). It is

FURTHER ORDERED, on the court's own motion, that appellees file a response, not to exceed 20 pages, by 12:00 noon, Friday, November 13, 2015, and that appellants file any reply by 12:00 noon, Monday November 16, 2015. The parties are directed to hand-deliver the paper copies of their submissions to the court by the time and date due.

Per Curiam