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.	)	Case No. 1:13-cv-851-RJL

THE GOVERNMENT DEFENDANTS' OPPOSITION TO PLAINTIFFS' RENEWED MOTION FOR A PRELIMINARY INJUNCTION

Dated: October 1, 2015

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

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 6102
Washington, D.C. 20044
Phone: (202) 514-3358
Fax: (202) 616-8470
E-mail: james.gilligan@usdoj.gov

TABLE OF CONTENTS

PAGE

PAGE

INTRODUCTION

Plaintiffs' renewed motion for a preliminary injunction presents very different questions for decision, under greatly changed circumstances, than did their initial motion two years ago. In June 2015 Congress enacted the USA FREEDOM Act, which brings to a close the NSA's bulk collection of telephony metadata under Section 215, but provides for a smooth transition to a new regime of targeted metadata collection by permitting the current program to operate until November 29, 2015, less than two months away. Plaintiffs have not demonstrated an entitlement to injunctive relief that would interfere with a FISC-supervised intelligence program that the Political Branches have determined remains necessary, in the interest of national security, until the new program of targeted collection is operationally ready to take its place.

As a threshold matter, the standing issue presented by this case has evolved following the ruling by the Court of Appeals. To support their standing, Plaintiffs initially relied on the inference that records of their calls must be collected under the Section 215 program because it could not effectively achieve its purposes unless it collected records from their provider. The Court of Appeals has now explained that such inferences are insufficient, under *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), to establish standing in a case of this kind. Plaintiffs, however, have not accepted this teaching. Instead they attempt to draw unsupported inferences, from unauthenticated documents, about which providers have participated in the program and when. They advance a claim that they subscribed to the services of an alleged participating provider "at all material times," without presenting evidence of specific facts to support it. Under the D.C. Circuit's ruling, these submissions do not meet the burden of proof that Plaintiffs must carry to establish their standing to seek preliminary injunctive relief.

The question whether Plaintiffs can demonstrate a likelihood of success on their Fourth Amendment claim has also evolved. Each court to consider similar challenges to the Section 215

program since this Court's December 2013 decision has ruled that such a claim is foreclosed by *Smith v. Maryland*, 442 U.S. 735 (1979). Even assuming, *contra Smith*, that Plaintiffs have a legitimate expectation of privacy in telephony metadata, they have not demonstrated an infringement of that interest, as is also necessary to sustain a Fourth Amendment claim.

Most significantly, since the Court issued its decision, Congress, acting on the initiative of the President, enacted the USA FREEDOM Act, Pub. L. No. 114-32, 129 Stat. 268. This legislation terminates bulk collection under Section 215 in favor of a targeted collection program designed to maintain the intelligence capabilities of the Section 215 program while providing even greater protections for individual privacy. The Act also provides for a six-month transition period, ending November 29, 2015, during which the Section 215 program may continue to operate while the technical infrastructure required for targeted collection is made operationally ready. The USA FREEDOM Act thus reflects the combined judgment of Congress and the President that NSA collection and analysis of bulk telephony metadata plays a valuable role in protecting the Nation from the threat of terrorist attack, and that the Government should retain this important intelligence capability until the new program of targeted collection can begin.

The USA FREEDOM Act fundamentally alters the Fourth Amendment reasonableness analysis in this case. Previously the Court held, notwithstanding the judicially mandated privacy protections already built into the Section 215 program, that the intrusion on privacy of indefinite bulk collection and long-term retention of telephony metadata, without prior judicial approval required for access to the data, outweighed the national-security interests served by the Section 215 program. Today, following the adoption of enhanced privacy protections initiated by the President and the transition provided for by the USA FREEDOM Act, the balance is dramatically different. Congress and the President have determined—in the midst of a terrorist threat environment that has also evolved over the past two years—that termination of the Section

215 program should not create an intelligence gap before the targeted collection program begins. There is no question that interim operation of the Section 215 program serves that important legislative goal. On the other side of the scale, increased privacy protections now part of the program—including greater judicial supervision by the Foreign Intelligence Surveillance Court (FISC)—and the program's imminent termination, have further minimized the potential for intrusion on Plaintiffs' privacy interests, in terms of both the finite duration of bulk collection (less than two months) and limited, FISC-approved access to the data. Under the circumstances that inform the special-needs analysis in this case today, the continued operation of the Section 215 program for another 60 days is reasonable, and therefore constitutional, under the Fourth Amendment.

The enactment of the USA FREEDOM Act recasts the public-interest analysis, and the balance of equities, in similar terms. Especially so in a case that implicates the Nation's security, a court must bear in mind the public consequences of awarding injunctive relief, and in considering where the public interest lies, must heed the judgment of Congress as expressed in legislation. The USA FREEDOM Act reflects the considered judgment of Congress that interim maintenance of the Section 215 program to combat the evolving threat of newly ascendant terrorist organizations outweighs the short-term potential for infringement on privacy interests. As explained below, an injunction that immediately barred collection of or access to telephony metadata under the Section 215 program, even if limited to records of just the Plaintiffs' calls, would effectively compel the NSA to cease all collection and analysis under the program before the targeted collection program can be made operational. That outcome would be contrary to the public interest in national security as Congress has defined it.

For all these reasons, explained more fully below, Plaintiffs' renewed motion for a preliminary injunction should be denied.

BACKGROUND

The Section 215 Bulk Telephony-Metadata Program

Plaintiffs seek an injunction against the final two months of the Government's FISC-authorized acquisition and analysis of bulk telephony metadata, conducted for purposes of discovering communications with and among unknown terrorist operatives. Since May 2006 this program has operated under authority of FISA's "business records" provision, 50 U.S.C. § 1861, enacted by Section 215 of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). Section 215 authorizes the Government to apply to the FISC for an order requiring the "production of any tangible things" . . . for an investigation," *inter alia*, "to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(a)(1). If the Government makes a showing "that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation," *id.* § 1861(b)(2)(A); *see id.* §§ 1861(a)(2)(A), (b)(2)(A), then the FISC "shall enter an ex parte order as requested, or as modified, approving the release of tangible things." *Id*. § 1861(c)(1).

Section 215 was "designed to ensure not only that the [G]overnment has access to the information it needs for authorized investigations, but also that there are protections and prohibitions in place to safeguard U.S. person information." *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, Dkt. No. BR 13-109, Am. Mem. Op. at 9 (F.I.S.C. Aug. 29, 2013) (publicly released, unclassified version) ("Aug. 29, 2013 FISC Op.") (Exhibit 1, hereto). Hence, in connection with a production order, the statute requires the Government to adopt and comply with FISC-approved procedures that "minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need . . . to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1861(b)(2)(B), (c)(1), (g)(2), (h).

Under the Section 215 bulk telephony-metadata program (briefly, the "Section 215 program"), the Government obtains FISC orders directing certain telecommunications service providers to produce business records of theirs known as "call-detail" records. Call-detail records contain information about telephone calls referred to as metadata—such as the date, time, and duration of a call and the dialing and receiving numbers—but not the substantive content of the call. Decl. of Teresa H. Shea, Signals Intelligence Director, NSA ("Shea Decl.") (Exhibit 2, hereto), ¶¶ 7, 13–15, 18 (Dkt. No. 25-4); *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR 15-99, Primary Order (F.I.S.C. Aug. 27, 2015) ("Primary Order") (Exh. 3, hereto) at 3 n.1. The FISC orders expressly exclude "the name, address, or financial information of a subscriber or customer," or any party to a call, from the definition of telephony metadata. Primary Order at 3 n.1. The FISC orders also do not permit the Government, under this program, to listen to or record the contents of conversations. Shea Decl. ¶¶ 7, 15. Under the FISC orders, the NSA's authority to continue the program expires after approximately 90 days and must be renewed. The FISC first authorized the program in May 2006, and since then has renewed the program 43 times, under orders issued by 19 different FISC judges. *See* Declaration of Major General Gregg C. Potter, Deputy Director, Signals Intelligence Directorate, NSA ("Potter Decl.") (Exhibit 4, hereto) ¶ 7.

Although the Government has acknowledged that the Section 215 telephony metadata program is broad in scope and involves the collection and aggregation of a large volume of data from multiple telecommunications service providers, the program has never captured information on all (or virtually all) calls made and/or received in the U.S. The FISC has also explained that the Government does not acquire call-detail records relating to all telephone calls to, from, or within the United States. Aug. 29, 2013 FISC Op. at 4 n.5 ("[P]roduction of all call detail records of all persons in the United States has never occurred under this program.").

The Government uses the telephony metadata it collects under this program to create a historical repository of information from multiple telecommunications networks that is then used to ascertain whether international terrorist organizations under investigation are communicating with operatives in the United States, for the purpose of detecting and preventing terrorist attacks. Shea Decl. ¶¶ 44–63; Aug. 29, 2013 FISC Op. at 18–22. As the program currently operates, when the FISC determines that there is reasonable, articulable suspicion that a selector, such as a telephone number, is associated with a terrorist organization being investigated by the Government, NSA analysts may then, and only then, conduct "contact chain" queries to obtain telephone numbers (or other metadata) that have been in contact within two steps, or "hops," of the suspected-terrorist selector (again, under the most recent FISC orders). Shea Decl. ¶¶ 26, 46–47. The Government uses query results in conjunction with a range of analytical tools to ascertain those contacts that may be of use in identifying individuals who may be associated with certain foreign terrorist organizations because they have been in communication with certain suspected-terrorist telephone numbers or other selectors. Shea Decl. ¶¶ 26–28.

The requirement of reasonable, articulable suspicion, known as "RAS," is a crucial minimization procedure that bars indiscriminate querying of the metadata based on selectors not connected with terrorist activity.[1] Because of this requirement, the vast majority of the data obtained under this program is never reviewed by any person. Shea Decl. ¶ 5. And when a RAS-based query is performed, the information it returns does not include the names or addresses of persons associated with the responsive telephone numbers, because that information is not included in the call-detail records that the providers produce. *Id.* ¶¶ 21, 43. Even where

[1] *See* Primary Order at 4 ("The government is hereby prohibited from accessing [business records] metadata . . . for any purpose except as described herein."); Aug. 29, 2013 FISC Op. at 5 n.7 ("A selection term that meets specific legal standards has always been required. This Court has not authorized government personnel to access the data for the purpose of wholesale 'data mining' or browsing."); 50 U.S.C. § 1861(c)(1) and (g).

query results reveal information bearing on one or more counter-terrorism investigations, FISC orders authorizing the program strictly prohibit the NSA from disseminating information concerning U.S. persons unless a senior NSA official determines the information is necessary to understand counter-terrorism information or assess its importance. Primary Order at 11-12.[2]

The Court's Ruling on Plaintiffs' Initial Motion for a Preliminary Injunction

Plaintiffs first moved for a preliminary injunction prohibiting bulk collection of metadata pertaining to their telephone calls on October 29, 2013 (*see* ECF No. 10), which the Court granted on December 16, 2013. *See Klayman v. Obama*, 957 F. Supp. 2d 1, 9-10 (D.D.C. 2013). In so ruling, the Court first concluded that Plaintiffs Klayman and Strange (but not their co-plaintiffs) had standing to challenge both the bulk collection of metadata under the Section 215 program and analysis of that data through the NSA's electronic querying process. The Court found that metadata pertaining to the telephone calls of Plaintiffs Klayman and Strange are likely collected under the program because they are subscribers to telephone service provided by Verizon Wireless, and the program, the Court reasoned, could not serve its function unless the NSA collected metadata in bulk from all of the top three wireless carriers, including Verizon Wireless. *Id.* at 26-27. The Court held that Plaintiffs Klayman and Strange also had standing to challenge the NSA's query process, reasoning that the NSA analyzes "*everyone's* metadata" when it runs queries of the data, whether records of their calls are retrieved or not. *Id.* at 27-28.

[2] To ensure compliance with these safeguards, the FISC's orders impose an extensive regime of internal reporting, audits, and oversight; regular consultation between the NSA Office of the Inspector General and the Department of Justice to assess compliance with FISC requirements; and monthly reports to the FISC including, *inter alia*, the number of times query results containing U.S. person information have been disseminated outside NSA. Shea Decl. ¶¶ 34-35. The Government has made public FISC orders and opinions concerning various failures to fully comply with these safeguards, owing to human error and technological issues, that were discovered in 2009. The Government reported these problems to the FISC (and Congress) and remedied them, and the FISC (after temporarily suspending the NSA's authority to query the database without court approval) reauthorized the program. *Id*. ¶¶ 36–43.

On the merits, the Court addressed whether the Section 215 program violates Plaintiffs' reasonable expectation of privacy. *Id.* at 30. The Court first determined that *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that individuals have no reasonable expectation of privacy in the telephone numbers they dial), does not control the Fourth Amendment question. The Court concluded that the collection and analysis of bulk telephony metadata under Section 215 is distinguishable from the pen-register recording of dialed telephone numbers in *Smith*, based on the Section 215 program's (then) indefinite duration, the Government's greater ability today to gather, store, and analyze telephony metadata about the calls of large numbers of individuals, and the greater variety and quantity of information about individuals that can be gleaned from such metadata today. *Klayman*, 957 F. Supp. 2d at 32-37. For essentially these reasons the Court also held that the Section 215 program violates Plaintiffs' expectation of privacy in aggregated metadata about their telephone communications. *Id.* at 37. Having thus concluded that the program involves a Fourth Amendment search, the Court next held that it does not meet the test of reasonableness under the Fourth Amendment "special needs" doctrine, finding that 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.

Turning finally to the remaining preliminary-injunction factors, the Court 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," *id.* at 42, and that providing relief to those two Plaintiffs alone would not be detrimental to the public interest in combating terrorism, *id.* at 43. The Court accordingly granted Plaintiffs Klayman's and Strange's request for a preliminary injunction, barring the Government from collecting, under the Section 215 program, any telephony metadata associated with their calls, and requiring the Government to destroy any such metadata in its possession. However, "in light

of the significant national security interests at stake" and the perceived novelty of the constitutional issues, the Court stayed its injunction pending the Government's appeal. *Id.*

All other federal courts to rule on the question have concluded that the Section 215 program is consistent with the Fourth Amendment. *See Smith v. Obama*, 24 F. Supp. 3d 1005, (D. Idaho 2014), *appeal pending*, No. 14-35555 (9th Cir.); *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *rev'd on other grounds*, 785 F.3d 787 (2d Cir. 2015); *United States v. Moalin*, 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013).[3]

The USA FREEDOM Act

On March 27, 2014, the President announced, after considering options presented by the Intelligence Community and the Attorney General, that he would seek legislation to replace the Section 215 program.[4] The President stated that his goal was to "establish a mechanism to preserve the capabilities we need without the [G]overnment 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." *Id.* Instead of the NSA obtaining telephony metadata in bulk, the President proposed that the data should remain in providers' hands, *id.*, and be produced to the NSA on a targeted basis only pursuant to orders from the FISC. The

[3] These include unanimous decisions by judges of the FISC. *See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, Dkt. Nos. BR 15-77, 15-78, at 19-25 (F.I.S.C. June 17, 2015) ("June 17, 2015 FISC Op."), http://www.fisc.uscourts.gov/sites/default/files/ BR%2015-77%2015-78%20Memorandum%20 Opinion.pdf; *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, Dkt. No. BR14-01, Op. and Order, 21-22 (FISC Mar. 20, 2014) ("Mar. 20, 2014 FISC Order)" (Exhibit 5, hereto); *see also In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, Dkt. No. BR13-109, Amended Mem. Op., 2013 WL 5741573 at *2-3 (FISA Ct. Aug. 29, 2013); *see also In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, Dkt. No. BR14-96, Mem. Op., at 11 (FISC. June 19, 2014), http://www.fisc.uscourts.gov/sites default/files/ BR%2014-96%20Opinion-1.pdf; *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, Dkt. No. BR13-158, Mem. Op, at 4-6 (FISA Ct. Oct 11, 2013 (McLaughlin J.) http://www.fisc.uscourts.gov/sites/default/files/BR%2013-158%20Memorandum-1.pdf.

[4] Statement by the President on the [Section 215] Program, http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program.

President stated that legislation would be needed to permit the NSA to obtain the data "with the speed and in the manner that [would] be required to make this approach workable." *Id.*[5]

Consistent with the President's objectives, on June 2, 2015, Congress enacted the USA FREEDOM Act, Pub. L. No. 114-22, 129 Stat. 268. The new statute will, beginning November 29, 2015, prohibit the Government from obtaining telephony metadata in bulk under Section 215. *See id.* §§ 103 & 109, 129 Stat. at 272, 276. In place of bulk collection under Section 215 Congress authorized a new mechanism providing for targeted production by service providers of call-detail records. *See id.* § 101, 129 Stat. 269-70. Congress also provided for a 6-month transition period by delaying for 180 days the effective date of the new prohibition on bulk collection under Section 215, and also the corresponding implementation date of the new regime of targeted production under the statute. *Id.* § 109(a), 129 Stat. at 276.

The design and effect of delaying the prohibition on bulk collection is to preserve 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) (noting the Government's understanding that the "USA FREEDOM Act would establish a 180-day transition period for transitioning from the current bulk-collection program for telephone

[5] By this time the President had already announced and the FISC had adopted two changes to the Section 215 program to enhance the substantial privacy protections already built into it. The first requires advance findings by the FISC, rather than designated NSA officials, of reasonable, articulable suspicion that a selector used to query the metadata is associated with an identified terrorist organization (except in emergency situations, in which case the Government must seek retrospective FISC approval of the selector). The second change limits query results to metadata within two "hops" of the suspected terrorist selector rather than three, as the FISC's orders previously allowed. These modifications have remained elements of the program embedded in the FISC's orders since that time. *See* Remarks by the President on Review of Signals Intelligence, http://www.whitehouse.gov/the-press-office/2014/01/17/ remarks-president-review-signals-intelligence; Potter Decl. ¶¶ 5-7.

metadata to a model where queries would be carried out against business records held by telephone service providers"). As the Government explained to Congress, 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 FISC for authorization to continue the Section 215 program during the transition period. After again carefully considering and rejecting the Fourth Amendment argument against the Section 215 program, the FISC granted that request, holding that Congress in the USA FREEDOM Act authorized the Government to continue the Section 215 program for 180 days as part of an orderly transition away from bulk collection of telephony metadata under that program. June 29 FISC Op. at 10-12 (*see supra*, at 9 n.3).

As indicated in the August 27 Primary Order, the FISC has taken under advisement whether to permit the NSA, after the transition period ends, to retain historical metadata collected under Section 215 prior to November 29, 2015, for purposes of (1) any applicable preservation obligations in still-pending litigation involving the Section 215 program, and (2) allowing technical personnel continued access for three months (until February 29, 2016) to verify that the production of call-detail records under the targeted collection program yields similar results to queries of metadata under the retiring bulk program. Potter Decl. ¶ 15; Aug. 27 Primary Order at 13; *Statement by the ODNI on Retention of Data Collected Under Section 215 of the USA PATRIOT Act*, http://icontherecord.tumblr.com/post/125179645313/ statement-by-the-odni-on-retention-of-data ("ODNI Statement"). Even if the FISC approves the retention of historical telephony metadata for these purposes, the Government has determined that analytic access to the data will cease at the end of the transition period; the data will not be used for

intelligence or law-enforcement purposes, and will not be disseminated. Following the three-month period of technical access, the historical telephony metadata will be retained "solely because of preservation obligations in pending civil litigation," and will be destroyed as soon as possible upon the expiration of such obligations." ODNI Statement; Potter Decl. ¶¶ 15-17.

The Court of Appeals' Decision

On August 28, 2015, the D.C. Circuit vacated the Court's preliminary injunction for the reasons stated in the separate opinions of Judges Brown, Williams, and Sentelle. *Obama v. Klayman*, 2015 WL 5058403, at *2 (D.C. Cir. Aug. 28, 2015) (per curiam). All panel members agreed that Plaintiffs had not adequately demonstrated their standing to support preliminary injunctive relief. *Id.* at *4 (Brown, J.); *id.* at *8 (Williams, J.); *id.* at *10 (Sentelle, J.).

Judge Williams first observed that Plaintiffs "lack direct evidence that records [of] their calls have actually been collected" under the Section 215 program. *Id.* at *5. He considered at length Plaintiffs' contention that the NSA must be collecting bulk data from Verizon Wireless (and therefore records about their calls) because the Section 215 program would be ineffective unless it collected data "from every large carrier such as Verizon Wireless." *See id.* at *5-7. But given that the Government has not confirmed or denied that Verizon Wireless has participated in the program, *see id*. at *5, and its representations that it has never collected "all, or even virtually all, call records" under the program, Judge Williams found Plaintiffs' claimed inference "inadequate to demonstrate a substantial likelihood of injury," *id.* at *6. This was especially so, Judge Williams observed, considering the Supreme Court's rejection of a similar inferential claim of standing in *Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138 (2013). *Id.* at *6-8.

Judge Sentelle "agree[d] with virtually everything in Judge Williams' opinion," except his conclusion that the case should be remanded instead of dismissed, *see id.* at *9, 10. Judge Sentelle emphasized that Plaintiffs "never in any fashion demonstrate that the [G]overnment is or

has been collecting [call-detail] records from their [carrier]," and that *Amnesty International's* rejection of inferences "comparable" to those Plaintiffs rely on "cuts strongly" against their likelihood of prevailing on standing. *Id.* at *9-10. While Judge Brown concluded that Plaintiffs had demonstrated a possibility that records of their calls are or have been collected under the program, they had not shown it was substantially likely, and therefore they "f[ell] short of meeting the higher burden of proof required for a preliminary injunction." *Id.* at *2, 4.[6]

Plaintiffs' Fourth Amended Complaint

Following the ruling by the Court of Appeals, Plaintiffs moved for and obtained leave to file a Fourth Amended Complaint (ECF No. 145-1) ("Fourth Am. Compl."); *see* Minute Entry (Sept. 16, 2015), in an effort to address the defects in their standing. As relevant here, the Fourth Amended Complaint amends Plaintiffs' prior complaint in two respects. First, it adds as plaintiffs Mr. J. J. Little and his law firm, J. J. Little & Associates, P.C., alleging that both Mr. Little and his firm are and at "[a]t all material times" have been subscribers of Verizon Business Network Services, Inc. ("VBNS"). Fourth Am. Compl. ¶ 18. Second, the Fourth Amended Complaint pleads additional facts intended to support Plaintiffs' allegation that Verizon Wireless is a participating telecommunications service provider in the Section 215 program. *Id.* ¶¶ 47-48.

After amending their complaint, Plaintiffs filed their renewed motion for a preliminary injunction against the Section 215 program on September 21, 2015, ECF No. 149, nearly ten years after the FISC first authorized the program, and only 68 days before the program's scheduled termination as mandated by Congress.

[6] On September 3, 2015, Plaintiffs filed a motion to expedite issuance of the Court of Appeals' mandate. Appellees-Cross-Appellants' Motion to Expedite Issuance of Mandate, *Klayman v. Obama*, Nos. 14-5004 *et al.* (D.C. Cir.) (Doc. No. 1571478). On September 17, 2015, the Government advised the Clerk of the Court for the D.C. Circuit that it did not intend to file a response to Plaintiffs' motion.

ARGUMENT

"A preliminary injunction is an extraordinary and drastic remedy; it is never awarded as of right." *Munaf v. Geren*, 553 U.S. 674, 689-90 (2008). The movant bears the burden of demonstrating "by a clear showing" that the remedy is necessary and that the prerequisites for issuance of the relief are satisfied. *Mazurek v. Armstrong*, 520 U.S. 968, 972 (1997); *Abdullah v. Obama*, 753 F.3d 193, 197 (D.C. Cir. 2014). "[P]laintiff[s] seeking a preliminary injunction must establish that [they are] likely to succeed on the merits, that [they are] likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in [their] favor, and that an injunction is in the public interest." *Winter v. NRDC*, 555 U.S. 7, 20 (2008); *Abdullah*, 753 F.3d at 197. "A positive showing on all four factors is required." *Bayer HealthCare, LLC v. FDA*, 942 F. Supp. 2d 17, 23 (D.D.C. 2013).[7]

Further, preliminary relief cannot issue based speculation or the mere "possibility of irreparable harm." *Winter*, 555 U.S. at 21-22. A preliminary injunction should issue only upon a showing that irreparable harm is "likely in the absence of an injunction." *Id.* at 22; *see Sherley*, 644 F.3d at 392-93. Finally, a court deciding a preliminary injunction motion "must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief," *Winter*, 555 U.S. at 24, and "should pay particular regard for the public consequences in employing the extraordinary remedy of injunction." *Id.*

I. PLAINTIFFS HAVE NOT DEMONSTRATED INJURY SUFFICIENT TO ESTABLISH THEIR STANDING, NOR SHOWN IRREPARABLE HARM.

Plaintiffs' request for preliminary injunctive relief must be denied because they have not shown injuries sufficient to sustain Article III standing, a jurisdictional defect in their case that

[7] Plaintiffs assume that these factors are assessed on a "continuum" or "sliding scale" basis, Pls.' Br. at 5, but, as this Court noted, *see* 957 F. Supp. 2d at 25 n.31, the "continued viability" of the sliding-scale approach after *Winter* has been called into question by the D.C. Circuit and this Court. *Sherley v. Sebelius*, 644 F.3d 388, 392-93 (D.C. Cir. 2011); *Jack's Canoes & Kayaks, LLC v. Nat'l Park Serv.*, 933 F. Supp. 2d 58, 76 (D.D.C. 2013).

precludes any likelihood of success on their claims. Likewise, Plaintiffs have not shown that they will suffer any irreparable harm absent an injunction, an equally insuperable bar to relief.

A. Plaintiffs Lack Standing and Therefore Cannot Show a Substantial Likelihood of Success on the Merits.

"The judicial power of the United States" is limited by Article III of the Constitution "to the resolution of 'cases' and 'controversies'," *Valley Forge Christian College v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464, 471 (1982), and a demonstration of a party's standing to sue "is an essential and unchanging part of the case-or-controversy requirement," *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). Standing is also an essential element of the "merits" on which parties seeking a preliminary injunction must show a substantial likelihood of success, *Klayman*, 2015 WL 5058403, at *5 (Williams, J.); *id.* at *9-10 (Sentelle, J.), because they "must have standing" for the court "to have subject matter jurisdiction over . . . [their] motion." *Dominguez v. Dist. of Columbia*, 536 F. Supp. 2d 18, 23-24 (D.D.C. 2008) (Leon, J.). The standing inquiry "has been especially rigorous when reaching the merits of the dispute would force [a court] to decide whether . . . action[s] taken by one of the other two branches of the Federal Government," especially "in the fields of intelligence gathering and foreign affairs," "was unconstitutional." *Amnesty Int'l*, 133 S. Ct. at 1147.

To establish Article III standing, Plaintiffs must show that they have suffered injury in fact, "an invasion of a legally protected interest," *Defenders of Wildlife*, 504 U.S. at 560, that is "concrete, particularized, and actual or imminent." *Amnesty Int'l*, 133 S. Ct. at 1147. A "threatened injury must be *certainly* impending to constitute injury in fact," whereas "allegations of *possible* future injury are not sufficient." *Id.* The alleged injury must also be "fairly traceable to the challenged action" and be "redressable by a favorable ruling." *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010). Because Plaintiffs must show that they have standing "with the manner and degree of evidence required at the successive stages of the litigation,"

Lujan, 504 U.S. at 561, they cannot now rely on mere allegations. Rather, at the preliminary injunction stage their burden "[is] no less than that required on a motion for summary judgment," and they must set forth by affidavit or other evidence "specific facts" establishing their standing. *Food & Water Watch, Inc. v. Vilsack*, 79 F. Supp. 3d 174, 186 (D.D.C. 2015); *see Cacchillo v. Insmed, Inc.*, 638 F.3d 401, 404 (2d Cir. 2011).

1. Plaintiffs have not shown a substantial likelihood that records of their telephone calls have been collected under the Section 215 program.

Plaintiffs have failed to adduce evidence of specific facts demonstrating that they have standing to challenge the Section 215 program. As before, Plaintiffs Larry Klayman and Charles Strange rely on their attestations that they have for many years been subscribers of cellular telephone service provided by Verizon Wireless. *See* Pls.' Br. at 15-16; Affidavit of Larry Klayman (Klayman Aff.) ¶ 3, ECF No. 13-2; Affidavit of Charles Strange (Strange Aff.) ¶¶ 2-3, ECF No. 13-3. But apart from the Government's acknowledgment that VBNS received an April 25, 2013, FISC Secondary Order, which expired on July 19, 2013, the identities of any other telecommunications service providers participating in the program at any time remain classified. Moreover, it remains the case that the program has never captured information on all (or virtually all) calls made and/or received in the United States. Potter Decl. ¶ 18. As held by the Court of Appeals, in the face of these representations by the Government the Plaintiffs' assumption that Verizon Wireless "must be" a participating carrier in the Section 215 program to make it effective is insufficient, under the standard of certainty required by *Amnesty International*, even to establish a "substantial likelihood" of standing at the preliminary injunction stage. *Klayman*, 2015 WL 5058403, at *6-9 (Williams, J.); *id.* at *9 (Sentelle, J.).

On remand, Plaintiffs Klayman and Strange now claim to offer proof that Verizon Wireless is one of the telecommunications companies from which the NSA currently collects telephony metadata in bulk. Pls.' Br. at 15. They refer, specifically, to Exhibit 1 to the Fourth

Amended Complaint, which purports to be a Government filing with the FISC in a proceeding that includes the company name "Verizon Wireless" (among others) in the caption. *See* Fourth Am. Compl. Exh. 1, at 1; Pls.' Br. at 15. This document does not support the conclusion, however, that Verizon Wireless is now or ever has been a participating telecommunications service provider in the Section 215 bulk telephony-metadata program.

As a threshold matter the document, apparently downloaded from the *New York Times* website, has not been authenticated, and the Government neither confirms nor denies its authenticity here. Thus, the document lacks evidentiary value. *Schwarz v. Lassen Cnty. ex rel. Lassen Cnty. Jail*, 2013 WL 5425102, at *10 (E.D. Cal. Sept. 27, 2013) (remarking that "evidence procured off the Internet is adequate for almost nothing" without authentication); *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F.Supp. 2d 773, 775 (S.D. Tex. 1999) (same).

Moreover, the extent to which Verizon Wireless (or any other carrier) has participated in the Section 215 program could not be deduced from the face of this document, even if it were genuine. The document does not state the nature of Verizon Wireless's (or any other carrier's) involvement in the proceeding, much less that Verizon Wireless (or any other carrier) was required to produce telephony metadata in bulk to the NSA.[8] Nor does the document specify the scope of the proceeding in question, and nothing stated therein suggests that the particular matters addressed in the filing involved activities in which Verizon Wireless participated.

Finally, the document is dated August 2, 2010, Fourth Am. Compl., Exh. 1, at 1, more than five years ago. As such, it has little to no probative value as to the current involvement of Verizon Wireless in the Section 215 program, if any. Thus, Plaintiffs Klayman and Strange still have adduced no competent evidence that Verizon Wireless is now participating or ever has

[8] Indeed, Exhibit 2 to the Fourth Amended Complaint, purportedly a New York Times article disclosing the alleged FISC document, itself observes that "it is not clear whether the inclusion of Verizon Wireless in the name of the court [filing] means it was turning over customer records after all." Fourth Am. Compl. Exh. 2, at 4.

participated in the Section 215 program. Whether that is in fact the case remains a matter of conjecture that the Court of Appeals has explained is insufficient, under the holding and analysis of *Amnesty International*, to establish that the NSA has collected telephony metadata pertaining to Plaintiffs' calls. *Klayman*, 2015 WL 5058403, at *6-10 (Williams and Sentelle, JJ.).

Like Plaintiffs Klayman and Strange, Plaintiffs J. J. Little and his law firm (together, the "Little Plaintiffs") also fail to carry their burden of setting forth "specific facts" that establish their standing. *Food & Water Watch*, 79 F. Supp. 3d at 186. Mr. Little attests that he and his firm "have been and are customers (subscribers) of [VBNS] at all material times relevant to the Fourth Amended Complaint." Pls.' Br., Exh. 1 ¶ 2. That statement simply echoes the allegation of the Fourth Amended Complaint that "[a]t all material times," the Little Plaintiffs "ha[ve] been and continue[ ] to be" subscribers of VBNS, Fourth Am. Compl. ¶ 18. Thus, Mr. Little's declaration falls short of establishing his or his firm's standing, for at least two reasons.

First, the Government has acknowledged that VBNS participated in the Section 215 bulk telephony-metadata program only for the duration of the FISC's April 25, 2013, Secondary Order, which expired on July 19, 2013. Whether or not VBNS has participated in the program at any other time remains a classified fact, *see* Potter Decl. ¶ 19, as to which Plaintiffs have adduced no evidence. Yet Mr. Little's bare assertion that he and his firm have been subscribers to VBNS telephone services "at all material times" is not sufficient to carry the Little Plaintiffs' burden of demonstrating that they were VBNS subscribers between April 25 and July 19, 2013. At this stage of the proceedings, where Plaintiffs' burden is to set forth specific facts supporting their standing, *Food & Water Watch*, 79 F. Supp. 3d at 186, they may not simply "replace conclusory allegations of [their] complaint . . . with conclusory allegations of an affidavit." *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 888 (1990); *see also Ass'n of Flight Attendants, CWA v. U.S. Dep't of Transp.*, 564 F.3d 462, 466 (D.C. Cir. 2009); *Uhuru v. U.S. Parole*

Comm'n, 734 F. Supp. 2d 8, 11 (D.D.C. 2010) (Leon, J.). Mr. Little's declaration proves (at most) only that he was a VBNS subscriber at the times *he* considers material, without providing the Court any independent basis on which to make that determination for itself.[9]

Second, even if Mr. Little's declaration were accepted as sufficiently specific evidence that the Little Plaintiffs "are [currently] customers . . . of [VBNS]," Pls.' Br. Exh. 1 ¶ 2, there is no evidence before the Court that VBNS is currently a participating provider in the Section 215 program. An 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 *Amnesty International* to establish a plaintiff's standing in a case of this nature. 2015 WL 5058403, at *7-8 (Williams, J.); *id.* at *10 (Sentelle, J.).

In short, it remains the case that no Plaintiffs here have established collection of records about their calls, and thus their standing, with the manner and degree of evidence required to obtain a preliminary injunction. *See Klayman*, 2015 WL 5058403, at *4 (Brown, J.) (concluding that even if Plaintiffs had "barely fulfilled the requirements for standing at this threshold stage, [they] [fell] short of meeting the higher burden of proof required for a preliminary injunction").

2. Even if collection of records about Plaintiffs' calls were presumed, Plaintiffs have demonstrated no resulting injury.

Even if it were assumed that the NSA has obtained third-party records about Plaintiffs' calls under the Section 215 program, to establish their standing Plaintiffs still would have to show that this action "inva[des] . . . a legally protected interest." *Defenders of Wildlife*, 504 U.S.

[9] This fact differentiates the standing question here from that in *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015). The plaintiff in *ACLU* 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. *ACLU v. Clapper*, No. 1:13-cv-03994 (S.D.N.Y.), Declaration of Steven R. Shapiro (ECF No. 29) ¶ 6. Hence, the Government did not contest the plaintiff's claim that records of its calls were among those collected under the program. *ACLU*, 785 F.3d at 801.

at 560. Plaintiffs' allegations in this regard are speculative and conjectural, not actual or imminent, as Article III requires. *Amnesty Int'l*, 133 S. Ct. at 1147. Plaintiffs Klayman and Strange express concern that information about their telephone calls allegedly collected by the NSA may be "used against" them in some manner, Klayman Aff. ¶ 10; Strange Aff. ¶ 11, but these unsubstantiated fears cannot support their standing in face of the established facts. Under FISC orders, NSA analysts may only review records responsive to queries using selectors the FISC has approved based on reasonable, articulable suspicion that they are associated with identified foreign terrorist organizations. *Supra*, at 6; Primary Order at 6–7; Potter Decl. ¶¶ 6-7. As a result, only a "tiny fraction" of the records is ever seen by any person. Shea Decl. ¶ 23. Plaintiffs present no evidence that the NSA has accessed records of their calls as a result of queries made under the "reasonable, articulable suspicion" standard or otherwise. Thus, it is conjecture to suggest that records of Plaintiffs' calls have been reviewed through such queries (much less that they will be during the remaining two months of the Section 215 program), or "used against" Plaintiffs in some unexplained way. Such a "speculative chain of possibilities" is not sufficient to establish Article III standing. *Amnesty Int'l*, 133 S. Ct. at 1148-50.[10]

The Court previously concluded, nonetheless, that Plaintiffs have standing to challenge the alleged analysis of metadata pertaining to their calls on the basis that queries of the database "necessarily analyze metadata for *every* phone number . . . to determine which U.S. phones, if any, have interacted with the target number." 957 F. Supp. 2d at 28. The Court concluded that this use of the NSA's Section 215 database "'implicates the Fourth Amendment each time a government official monitors it,'" in the same manner as Government monitoring of the

[10] Plaintiffs' related assertions that the Section 215 program has "directly and significantly impacted" their "ability to communicate via telephone," and to engage in public advocacy, Klayman Aff. ¶¶ 9-10; Strange Aff. ¶¶ 11, 19-20, simply reflect their unsubstantiated fears that the NSA will misuse data about their calls, fears that are insufficient to establish Article III injury. *Amnesty Int'l*, 133 S. Ct. at 1152; *Laird v. Tatum*, 408 U.S. 1, 10, 14 (1972); *United Presbyterian Church in the USA v. Reagan*, 738 F.2d 1375, 1378 (D.C. Cir. 1984).

hypothetical home video camera discussed in *Johnson v. Quander*, 440 F.3d 489 (D.C. Cir. 2006). *Id.* at 28-29. The analogy, however, is not apt.

Johnson explained that an in-home video camera would raise Fourth Amendment concerns each time it is monitored by a government official because each such time the camera reveals new and otherwise private information about the homeowner to that official. 440 F.3d at 498–99. The same cannot be said regarding NSA queries of bulk telephony metadata obtained under Section 215. When the NSA runs such queries its analysts see no metadata associated with anyone's calls, and thus learn no information about the communications of any individuals, unless their telephone numbers (or other identifiers) fall within two "hops" of a suspected terrorist selector. *See* Shea Decl. ¶¶ 22-24; Potter Decl. ¶ 6.

Instead, the instructive precedents here are the Supreme Court's decisions in *United States v. Place*, 462 U.S. 696, 707 (1983), *United States v. Jacobsen*, 466 U.S. 109, 123 (1984), and *United States v. Karo*, 468 U.S. 705 (1984). In *Place*, DEA agents took a suspect's luggage from his possession and transported it to another location for a "sniff test" by a trained narcotics-detection dog. The dog alerted to one of the bags, and the agents, upon obtaining a search warrant, opened the bag and discovered cocaine inside. 462 U.S. at 698-99. Although ultimately concluding that Place's luggage had been unconstitutionally seized, the Supreme Court first concluded that subjecting the luggage to the canine sniff test did not constitute a Fourth Amendment search. The Court explained:

> A "canine sniff" by a well-trained narcotics detection dog . . . does not require opening the luggage. *It does not expose noncontraband items that otherwise would remain hidden from public view*, as does, for example, an officer's rummaging through the contents of the luggage. Thus, the manner in which information is obtained through this investigative technique is much less intrusive than a typical search. Moreover, the sniff discloses only the presence or absence of narcotics, a contraband item. Thus, despite the fact that the sniff tells the authorities something about the contents of the luggage, the information obtained is limited.

Id. at 707 (emphasis added).

The Court extended the logic of *Place* to a chemical test for narcotics in *Jacobsen*. In that case, upon the mid-shipment discovery of a white powdery substance inside a damaged parcel, DEA agents performed an "on the spot" chemical field test that identified the substance as cocaine, leading to the arrest and conviction of the package's intended recipients. 466 U.S. at 111-12 & n.1. The Court held that the chemical test did not constitute a Fourth Amendment search, because it "could disclose only one fact . . . whether or not a suspicious white powder was cocaine"—"nothing more"—and therefore "d[id] not compromise any legitimate interest in privacy." *Id.* at 122-23. "[E]ven if the results are negative," the Court emphasized, "such a result reveals nothing of special interest," because the chemical test, like a narcotics-dog sniff, "could reveal nothing about noncontraband items." *Id.* at 123-24 & n.24.

The Court applied a like analysis in *Karo*, and reached a like result. In *Karo* DEA agents placed an electronic tracking device among cans of ether the defendant had purchased for suspected purposes related to drug trafficking. 468 U.S. at 708. Ultimately, the Court held that use of the tracking device to locate the ether at the defendant's place of residence violated his Fourth Amendment rights. *Id.* at 709-10, 714-15. But it also held as a threshold matter that the initial placement of an active electronic tracking device among the cans of ether infringed no privacy right of the defendant, because until the device was actually monitored by DEA agents it "conveyed no information that [the defendant] wish[ed] to keep private, *for it conveyed no information at all.*" *Id.* at 712 (emphasis added).

The logic underlying *Jacobsen*, *Place*, and *Karo* applies equally to queries of the metadata that retrieve no records of Plaintiffs' calls. So long as records of Plaintiffs' calls are not among the tiny fraction of records responsive to analysts' queries, electronic queries of the database "convey no information at all" about them to human analysts. *Id.* Therefore, absent some indication that NSA analysts conducting queries of the database have retrieved and

reviewed records containing metadata associated with Plaintiffs' calls, they cannot demonstrate that the query process itself constitutes an "*invasion* of a legally protected interest," *Defenders of Wildlife*, 504 U.S. at 560 (emphasis added), even assuming, *contra Smith v. Maryland*, 442 U.S. 735 (1979), that they have a protected privacy interest in telephony metadata to begin with.[11]

Plaintiffs have presented no evidence of specific facts demonstrating with the rigor required in this context, *Amnesty Int'l*, 133 S. Ct. at 1147, 1149, that they have standing to contest the NSA's collection or querying of bulk telephony metadata under Section 215. Plaintiffs' motion for a preliminary injunction must therefore be denied.

B. Plaintiffs' Speculative Injuries Also Do Not Establish Irreparable Harm.

To satisfy the "high standard" for establishing irreparable harm, *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 297 (D.C. Cir. 2006), Plaintiffs must show that their asserted injuries are "certain" and "great," not "theoretical," and "of such *imminence* that there is a 'clear and present' need" for relief to prevent this harm that would otherwise be "beyond remediation." *Stand Up for California! v. U.S. Dep't of the Interior*, 919 F. Supp. 2d 51, 81

[11] Reinforcing this conclusion are *Horton v. California*, 496 U.S. 128, 142 n.11 (1990) (government's acquisition of item without examining its contents "does not compromise the interest in preserving the privacy of its contents") and *United States v. Van Leeuwen*, 397 U.S. 249, 253 (1970) (defendant's interest in privacy of detained first-class mail "was not disturbed or invaded" until the Government opened the packages). The Court in *Klayman* described the above-quoted language from *Horton* and *VanLeeuwen* as dicta, 957 F. Supp. 2d at 29 n.40, but they are in fact statements of the law. *See, e.g.*, *United States v. Banks*, 3 F.3d 399, 401-02 (11th Cir. 1993) ("no Fourth Amendment privacy interest in first-class mail is invaded by detaining such mail . . . until a search warrant can be obtained," because "the privacy interest in the packages" was not disturbed); *United States v. Licata*, 761 F.2d 537, 541 (9th Cir. 1985) (seizure of a closed container "affects only the owner's possessory interests and not the privacy interests vested in the contents"). *See also Texas v. Brown*, 460 U.S. 730, 748-49 (1983) (Stevens, J., concurring in the judgment); *United States v. Clutter*, 674 F.3d 980, 984 (8th Cir. 2012) (seizure of computers, later found to contain child pornography, did not implicate Fourth Amendment privacy interests at time seizure occurred). In addition, while the Court previously rejected the locked-container analogy because "all of the metadata is handled by the Government *at least* to the degree needed to integrate the metadata into the NSA's database," 957 F. Supp. 2d at 29 n.40, the FISC's Orders prohibit technicians from sharing information from the results of such purely technical access for intelligence analysis purposes. *See* Aug. 27, 2015 Primary Order at 6.

(D.D.C. 2013). It follows *a fortiori* from Plaintiffs' failure to demonstrate that they have suffered a sufficiently concrete injury to establish standing, that they have failed to show they are "likely to suffer irreparable harm before a decision on the merits can be rendered." *Id.*[12]

II. PLAINTIFFS WILL NOT LIKELY SUCCEED ON THE MERITS OF THEIR FOURTH AMENDMENT CLAIM.

Even if Plaintiffs had established their standing, the legal foundation of their Fourth Amendment claim—that they have a reasonable expectation of privacy in the numbers dialed to connect a telephone call (and other metadata)—is foreclosed by *Smith v. Maryland*, 442 U.S. 735 (1979), as every other court to address the question has held. *Smith*, and the third-party doctrine on which it relies, remain the law today. The factual differences between *Smith* and the telephony metadata program are immaterial to the reasoning of *Smith*, as the FISC explained in an opinion disagreeing with the Court's reasons in its prior preliminary injunction ruling, 957 F. Supp. 2d at 32-37, for declining to follow *Smith*. *See* Mar. 20, 2014 FISC Order. Even if there were a reasonable expectation of privacy in telephony metadata, contrary to *Smith*, Plaintiffs have not established an invasion of that interest. Moreover, Congress's decision to permit continued NSA bulk collection of telephony metadata for a brief transition period, until the program of targeted collection is fully operational, is constitutional, because it is reasonable under the standard applicable to searches that serve special needs of the Government.

[12] Further exposing the Little Plaintiffs' lack of irreparable harm is their more than two-year delay in seeking preliminary injunctive relief. *See Gordon v. Holder*, 632 F.3d 722, 725 (D.C. Cir. 2011); *see also Brown v. Dist. of Columbia*, 888 F. Supp. 2d 28, 33 (D.D.C. 2012) (Leon, J.) (finding that plaintiff's six-month delay in seeking injunctive relief "directly undercuts any argument that her injury is of such imminence that there is a clear and present need for equitable relief to prevent irreparable harm"). The NSA's bulk telephony-metadata program became a widespread matter of public knowledge and was officially acknowledged by the Government in June 2013, following the publication by *The Guardian* of classified information obtained from former NSA contractor Edward Snowden. Yet without explanation the Little Plaintiffs waited for more than two years, until the program's waning days, to seek injunctive relief. This is yet another reason why this Court "should be reluctant to award relief." *NRDC v. Pena*, 147 F.3d 1012, 1026 (D.C. Cir. 1998).

A. Plaintiffs Have no Protected Privacy Interest in Telephony Metadata.

Since the decision in *Katz v. United States*, 389 U.S. 347 (1967), it has been understood that a Fourth Amendment "search" takes place not only when the government trespasses on areas, "persons, houses, papers, and effects," enumerated by the Fourth Amendment, but also when governmental investigative activities "violate a person's 'reasonable expectation of privacy.'" *Jones*, 132 S. Ct. at 949-50 (quoting *Katz*, 389 U.S. at 360).[13] The Supreme Court squarely held in *Smith*, however, that individuals have no reasonable expectation of privacy in the mere telephone numbers they dial because they knowingly give that information to telephone companies when they dial the numbers; the government's acquisition of such numbers did not therefore constitute a search under the Fourth Amendment. *Smith*, 442 U.S. at 741-46.

In *Smith*, the police requested (without a warrant or court order) that the telephone company install a pen register device at its central offices to record the numbers dialed from a robbery suspect's (Smith's) home phone. *Id.* at 737. After Smith was arrested, he sought to suppress evidence derived from the pen register, arguing that use of the pen register violated his Fourth Amendment rights. Contrasting the collection of the numbers dialed with the acquisition of the contents of communications at issue in *Katz*, *id.* at 741, the Court held that even if Smith harbored a subjective expectation that the phone numbers he dialed would remain private, that expectation was not reasonable.[14]

---

[13] The Government's collection of bulk telephony metadata pursuant to orders of the FISC does not constitute a "seizure" of individual subscribers' records, because the orders are directed to telecommunications service providers, not to subscribers, and direct the production of what are indisputably the providers' own business records. *See Klayman*, 957 F. Supp. 2d at 30 n.4. *See also Segura v. United States*, 468 U.S. 796, 806 (1984); *Smith*, 442 U.S. at 741; *United States v. Miller*, 425 U.S. 435, 440-41 (1976). As in their first preliminary injunction motion, Plaintiffs again "have not offered any theory as to how they would have a possessory interest" in data associated with their calls "held by Verizon." *Klayman*, 957 F. Supp. 2d at 30 n.41.

[14] Notwithstanding the holding in *Smith*, Plaintiffs rely on Verizon's "Privacy Policy" to claim that "telephone company subscribers absolutely do expect . . . telephone call metadata . . .

The Court explained that it "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44 (citing, *inter alia*, *Miller*, 425 U.S. at 441-43 (no reasonable expectation of privacy in financial records a depositor voluntarily provided to his bank)). Telephone users "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." *Id*. at 743. By using his phone, Smith "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," and therefore "assumed the risk that the company would reveal to police the numbers he dialed." *Id.* at 744; [15] *see also id*. at 745; *Miller*, 425 U.S. at 443 ("[D]epositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").[16]

---

will be kept secret and their confidences will be held inviolate by the telephone company." Pls.' Br. at 22. But in addition to the fact that this argument is foreclosed by law, *see Smith*, 442 U.S. at 745 (refusing to create a "crazy quilt" of Fourth Amendment protections that would ebb and flow based on individual corporate policies), it also has no factual support. Verizon's policy, beyond explaining the many ways in which Verizon has unilaterally determined it will collect, use, and store customer information, including "call records," and share it with various entities, also specifically advises customers that it "may disclose information that individually identifies [its] customers . . . in certain circumstances, such as . . . to comply with valid legal process including subpoenas, court orders." Verizon Privacy Policy, https://www.verizon.com/about/privacy/policy/#3rdparty. Verizon's privacy policy thus cannot be a source of a reasonable expectation of privacy that call detail records will not be turned over to the Government pursuant to a court order when the policy itself says just the opposite.

[15] As the FISC has observed, "a telephone user who is making a call fully divulges to the phone company the numbers he dials," unlike the bus passenger in *Bond v. United States*, 529 U.S. 334, 338 (2000), cited in *Klayman*, 957 F. Supp. 2d at 33 n.47, who sought to preserve the privacy of the contents of his carry-on bag by using an opaque bag and placing that bag directly above his seat. *See* Mar. 20, 2014 FISC Order at 16 n.8.

[16] The third-party doctrine has consistently been applied to call detail records like the business records at issue here. *See U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 454 (D.C. Cir 2000); *Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1043-46 (D.C. Cir. 1978); *United States v. Baxter*, 492 F.2d 150, 167 (9th Cir. 1973); *United States v. Fithian*, 452 F.2d 505, 506 (9th Cir. 1971); *United States v. Doe*, 537 F. Supp. 838, 839-40 (E.D.N.Y. 1982).

Therefore, *Smith* controls the instant case because the pen-register metadata at issue in *Smith* are "indistinguishable" from the non-content telephony metadata obtained through the challenged program, and so its rationale is fully applicable. *See* Mar. 20, 2014 FISC Order at 11; *Moalin*, 2013 WL 6079518, at *6-8. *See also Agostini v. Felton*, 521 U.S. 203, 237 (1997) (lower courts should "follow the case which directly controls, leaving to [the Supreme] Court the prerogative of overruling its own decisions").

B. *Smith* is not Distinguishable from this Case.

The Government recognizes that this Court concluded otherwise when it decided Plaintiffs' first motion for a preliminary injunction, but respectfully submits, for the reasons explained herein, and by all other courts to reach the Fourth Amendment issue presented here, that the factual differences between this case and *Smith* are immaterial to *Smith's* reasoning—that an individual has no reasonable expectation of privacy in information provided to third parties.[17]

First, the Section 215 program cannot be distinguished from *Smith* based on the Government's more extensive collection and longer retention of metadata pertaining to each individual's calls. *See* Pls.' Br. at 25; *Klayman*, 957 F. Supp. 2d at 32. *Miller*, on whose central holding *Smith* relied, upheld in the face of a Fourth Amendment challenge the compelled production of almost four months of a person's bank records—copies of checks, deposit slips, financial statements, monthly statements—that are more substantive and personal in nature than phone numbers, and more likely to reveal details about an individual's life than years' worth of telephony metadata. *See* Mar. 20, 2014 FISC Order at 21-22. Moreover, it is no longer likely true that the NSA will maintain a database "containing *five years'* worth of data" with the "very real prospect that the program will go on . . . forever!" *Klayman*, 957 F. Supp. 2d at 32. The

[17] Plaintiffs' reliance on the law-of-the-case doctrine, *e.g.*, Pls.' Br. at 2-3, is misplaced. The law-of-the-case doctrine does not apply to interlocutory orders, *Sloan v. Urban Title Servs., Inc.*, 770 F. Supp. 2d 216, 224 (D.D.C. 2011), such as preliminary injunctions, *see Decatur Liquors, Inc. v. Dist. of Columbia*, 2005 WL 607881, at *2 (D.D.C. March 16, 2005).

bulk telephony metadata program will end on November 29, 2015, *see* USA FREEDOM Act §§ 103, 109, and the Government has already announced that it will cease analytic access to the metadata immediately thereafter (assuming the FISC permits retention of the data at all) and to destroy the historical telephony metadata "as soon as possible . . . upon expiration of its litigation preservation obligations." *ODNI Statement*, *supra* at 11.[18]

Second, perceived distinctions between the relationship of the Government with the telephone company in *Smith*, and the relationship of the Government here with the providers that participate in the program, *see* Pls.' Br. at 25-26; *Klayman*, 957 F. Supp. 2d at 32-33, are simply irrelevant to whether a search occurred. Mar. 20, 2014 FISC Order at 17–18. Nor is there support in the record for the conclusion that the telecommunications companies that receive Section 215 orders are collecting telephony metadata for law enforcement purposes, "operat[ing] what is effectively a joint intelligence-gathering operation with the Government." *Klayman*, 957 F. Supp. 2d at 33.[19] 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)." Shea Decl. ¶ 18. *See also* Mar. 20, 2014 FISC Order at 18 n.9.

[18] And, while the volume of data collected and retained about an individual's phone calls is greater here than in *Smith*, the privacy concerns were actually greater in *Smith* because there the police targeted the phone calls of a single, known individual, examined the data gathered to ascertain whether he had contacted another known individual, and used that information to arrest and prosecute him. 442 U.S. at 737. Here, Plaintiffs have not shown that any metadata of their phone calls have ever been examined by NSA analysts, so Plaintiffs can complain of no putative invasion of privacy of the kind experienced by the criminal suspect in *Smith.*

[19] Notably, *Miller* rejected a similar argument that banks producing financial records to law enforcement were acting as government agents. 425 U.S. at 443. Also, this Court's comparison of the Government's relationship with providers here to the hospital's relationship with law enforcement in *Ferguson v. City of Charleston*, 532 U.S. 67 (2001), *see Klayman*, 957 F. Supp. 2d at 33, overlooks the fact that *Ferguson* did not involve a voluntary disclosure of information to a third party. The case was decided on the assumption that the patients did not consent to the disclosure, and the disclosure was made to state-hospital employees acting in collaboration with local law enforcement authorities. *See Ferguson*, 532 U.S. at 76, 78 n.13, 85.

Third, the Court also emphasized that the Section 215 program allegedly involves the collection of data "on hundreds of millions of people." Pls.'Br. at 26; *Klayman*, 957 F. Supp. 2d at 33 & n.48, 34, 36. That observation "is misplaced under settled Supreme Court precedent," Mar. 20, 2014 FISC Order at 19–20, however. Fourth Amendment rights "are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched." *Steagald v. United States*, 451 U.S. 204, 219 (1981); *accord Rakas v. Illinois*, 439 U.S. 128, 133–34 (1978). No Fourth Amendment interest of Plaintiffs is implicated, therefore, by the fact that the metadata of many other individuals' calls are collected as well as (allegedly) their own.[20]

Finally, the Court suggested that individuals' reasonable expectation of privacy is affected by the "ubiquit[y]" of cell phones and their many applications in modern life, which did not exist in 1979 when *Smith* was decided. *See Klayman*, 957 F. Supp. 2d at 36. As an initial matter, courts have continued to apply the third-party doctrine to non-content information generated by such digital-age necessities as connecting to the Internet, *see, e.g.*, *United States v. Christie*, 624 F.3d 558, 573 (3d Cir. 2010) (no reasonable expectation of privacy in subscriber information provided to Internet Service Provider); *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (same); *Guest v. Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001), communicating by email, *United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008) (no reasonable expectation of privacy in email addressing information), and sending text messages, *see Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 905 (9th Cir. 2008), *rev'd on other*

[20] *See United States v. Dionisio*, 410 U.S. 1, 13 (1973) (where single grand jury subpoena did not effect an unreasonable seizure, it was not "rendered unreasonable by the fact that many others were subjected to the same compulsion"); *In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987) ("[T]he fourth amendment does not necessarily prohibit the grand jury from engaging in a 'dragnet' operation."); *United States v. Rigmaiden*, 2013 WL 1932800, at *13 (D. Ariz. May 8, 2013) (Government did not violate defendant's Fourth Amendment rights by collecting a high volume (1.8 million) of IP addresses); Aug. 29, 2013 FISC Op. at 8–9.

grounds, 560 U.S. 746 (2010) (no reasonable expectation of privacy in text message addressing information).

Moreover, the use of banks, credit cards, telephones, and the like, to conduct the affairs of life was clearly prevalent in 1979, as both *Smith* and *Miller* demonstrate, and as the dissent in *Smith* expressly argued. *See* 442 U.S. at 749–50 (Marshall, J., dissenting). And while it is true that cell phones did not exist in 1979, and that cell phones are used for purposes other than making telephone calls (such as accessing the Internet, taking pictures, and text messaging), *see Klayman*, 957 F. Supp. 2d at 34-36, "none of these additional functions generates any information that is being collected by NSA as part of the telephony metadata program, which . . . involves only non-content records concerning the placing and routing of telephone calls. Accordingly, such changes are irrelevant . . ." Mar. 20, 2014 FISC Order at 19. *See also Klayman*, 957 F. Supp. 2d at 35 (acknowledging that the information acquired under the telephony metadata program is "limited" to "phone numbers dialed, date, time, and the like").[21]

Nor does *Jones* provide any basis for departing from the controlling authority of *Smith*. *See Klayman*, 957 F. Supp. 2d at 36; Pls.' Br. at 24. As the FISC explained, the majority opinion in *Jones*, in holding that an individual has a protected Fourth Amendment interest against the police attaching a GPS tracker to his car, relied on the "physical intrusion" the tracker effected and "declined to address the question whether use of the GPS device, without the physical intrusion, impinged upon a reasonable expectation of privacy . . . ." Mar. 20, 2014 FISC Order at 24-25. This Court placed reliance on Justice Sotomayor's concurring opinion for the proposition that "the metadata from each person's phone 'reflects a wealth of detail about her

[21] The Court has noted a "few . . . distinctions between the data at issue in *Smith* and the metadata that exists nowadays," *Klayman*, 957 F. Supp. 2d at 35 n.57. While those data (created by the provider) include "whether calls were completed" and the "duration of [those] calls," *id*, they do not alter the applicability of the third-party doctrine. *See United States v. Reed*, 575 F.3d 900, 914 (9th Cir. 2009); *United States Telecom Ass'n*, 227 F.3d at 454, 459.

familial, political, professional, religious, and sexual associations.'" *Klayman*, 957 F. Supp. 2d at 36.[22] But the Court in *Smith* was aware that a list of telephone numbers dialed "could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life," 442 U.S. at 748 (Stewart, J., dissenting), and it ruled that there is no reasonable expectation of privacy in the numbers dialed. Indeed, the potential for intrusion into the "most intimate details of a person's life" is far less here than in *Jones*, where law enforcement officers attached a GPS device to a single, known person's vehicle, recorded the vehicle's locations over a period of time, and then used that information to prosecute him. The telephony metadata at issue here do not contain the name or address of an individual, and the Government may only seek to find out that information for phone numbers that are returned as results of FISC-authorized queries. And here, of course, Plaintiffs offer no proof that any metadata of their calls have been reviewed by the Government.

* * * * * *

Thus, *Smith* compels the conclusion that the alleged acquisition of metadata records about Plaintiffs' telephone calls does not constitute a search for purposes of the Fourth Amendment, thereby ending the Fourth Amendment inquiry. But even if the Court concluded, contrary to *Smith*, that Plaintiffs have a reasonable expectation of privacy in metadata allegedly obtained about their phone calls, they point to no *invasion* of that interest that would rise to the level of a Fourth Amendment search. Contrary to this Court's prior conclusion, *see Klayman*, 957 F. Supp. 2d at 27-29, call detail records are not "searched" in a constitutional sense each time an electronic query of the database is performed. When such queries are conducted, the

[22] The *Jones* majority opinion is, of course, controlling, and does not undermine the vitality of *Smith* in any way. Moreover, although Justice Sotomayor stated in her concurring opinion that it may be necessary to reconsider the third-party doctrine, she expressly concluded that "[r]esolution of these difficult questions in this case is unnecessary . . . because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision." *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring). *See also* Mar. 20, 2014 FISC Order at 28.

only information made available for review by human beings are the records within two hops of the suspected terrorist selectors used to initiate the queries; NSA analysts receive no information about the calls of any other individuals. *See* Shea Decl. ¶¶ 20–26. Thus, as discussed above, *see supra*, at 22-24, the query process is analogous, in Fourth Amendment terms, to a canine sniff of luggage or chemical test for narcotics that exposes no non-contraband items to law enforcement officials, *see Place*, 462 U.S. at 707; *Jacobsen*, 466 U.S. at 123, or a tracking device that, because it is unmonitored, "convey[s] no information at all" to government agents. *Karo*, 468 U.S. at 712. None constitutes a "search" within the meaning of the Fourth Amendment; nor do electronic queries of the bulk metadata that return no records of Plaintiffs' telephone calls.

Accordingly, because Plaintiffs have not presented evidence that information associated with any of their phone calls has been reviewed by analysts in response to queries of the bulk telephony metadata collected by the NSA, they cannot maintain that NSA queries of the database intrude upon any putative expectation of privacy they claim to have in that information.

C. Continuing the Section 215 Program for Two Additional Months, Until the Targeted Collection Program Envisioned by the USA FREEDOM Act Is Operational, Is Reasonable Under the Fourth Amendment.

Even assuming that the Section 215 program infringed upon a legitimate expectation of privacy in telephony metadata, Plaintiffs' Fourth Amendment claim nevertheless would fail, because Congress's decision to permit continued operation of the Section 215 program for the time remaining until preparations for the NSA's new targeted program of collection are completed is reasonable under the Fourth Amendment's "special needs" doctrine.

The Supreme Court has recognized various exceptions to the warrant requirement, including where "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). 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). [23]

Since this Court last addressed the special-needs analysis in this case, several developments have weighted this balance still further in the Government's favor. The Section 215 program will expire on November 29. *See supra*, at 10; USA FREEDOM Act §§ 103, 109. Thus, while previously the Court had to weigh the Government's interests against a claimed intrusion on Plaintiffs' privacy of indefinite duration, the USA FREEDOM Act has transformed the task into weighing the Government's national-security interests against any intrusion on Plaintiffs' privacy occurring *over the next two months*. This development, as well as the additional executive and judicial modifications to the program described above, and the evolving terrorist threat environment over the past two years, make clear that continued operation of the Section 215 program for the next two months serves overriding public interests that outweigh the at-most minimal intrusions on Plaintiffs' privacy interests that could occur during that time.

The Section 215 program undoubtedly serves special Government needs above and beyond law enforcement. The purpose of the program—identifying unknown terrorist operatives and preventing terrorist attacks—is undisputed and weighty, as this Court recognized. *See Klayman*, 957 F. Supp. 2d at 39 (agreeing that "identifying unknown terrorist operatives and preventing terrorist attacks" is an interest "'of the highest order of magnitude'"). Such goals are forward-looking and fundamentally differ from most criminal law enforcement, which typically focuses on solving crimes that have already occurred, rather than preventing unlawful activity and protecting national security. *See, e.g., United States v. U.S. Dist. Court (Keith)*, 407 U.S.

[23] The Supreme Court has permitted warrantless stops at roadblocks to secure borders, *United States v. Martinez-Fuerte*, 428 U.S. 543, 566-67 (1976), warrantless searches of probationers' homes to ensure compliance with probation conditions, *Griffin*, 483 U.S. at 872-75, and warrantless searches of public school students to enforce rules, *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985), under the special needs doctrine.

297, 322-32 (1972); *In re Sealed Case*, 310 F.3d 717, 746 (FISC-R 2002); *see also NTEU v. Von Raab*, 489 U.S. 656, 668 (1989) ("traditional probable-cause standard may be unhelpful" when the Government "seeks to *prevent*" dangers to public safety); *Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006) (interest in preventing terrorist attacks goes "well beyond" law enforcement).

The enactment of the USA FREEDOM Act confirms the important contribution that the Section 215 program makes to the Nation's security. The Act reflects the combined judgment of Congress and the President that the program's capabilities should in the interests of national security be maintained—albeit under a new statutory framework involving targeted collection of metadata, to enhance public confidence that their privacy is being protected. By delaying the prohibition on bulk collection for 180 days, Congress also sought to ensure that the Government retained this capability until the targeted collection program could be made operational, to avoid creating an intelligence gap in the midst of the continuing terrorist threat. The interim operation of the Section 215 program unquestionably serves this important legislative objective.

The recent evolution of the terrorist threat environment underscores the immediacy and importance of the purposes served by Section 215 program during the transition period. "Over the past two years the United States has confronted . . . an increasing threat of attacks by individuals who act in relative isolation or in small groups," with the Islamic State of Iraq and the Levant ("ISIL"), as well as al-Qaida in the Arabian Peninsula" ("AQAP") both calling for these kinds of attacks against "the United States, its people, and its interests abroad." Declaration of Bryan Paarmann, Deputy Assistant Director, Counterterrorism Division, FBI ("Paarman Decl.") (Exhibit 6, hereto) ¶¶ 5-6. Due to the nature of these type of attacks, planning and coordination can be so "swift[]" that the participants "may leave fewer clues for investigators who are attempting to prevent or disrupt them." *Id.* ¶ 7. In addition, "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." *Id.* ¶ 8.

"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." *Id.* ¶ 9; *see United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980) ("[A]ttempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy."). Analysis of telephony metadata to *quickly* detect contacts of known or suspected terrorists is an important component of the Government's counter-terrorism arsenal, and "the current terrorist threat environment underscores the significance of this key capability under the NSA's bulk telephony metadata program." *Id.* ¶ 11. In short, the bulk telephony metadata program is a "reasonably effective means" of advancing the Government goal, *see Board of Education of Independent School District No. 92 v. Earls*, 536 U.S. 822, 837-38 (2002), of preventing terrorist attacks, 50 U.S.C. § 1861(a)(1), until the targeted collection program envisioned by the USA FREEDOM Act is operational.[24]

Balanced against the important purposes served by the Section 215 program during the transition period is the minimal impact the program will have on Plaintiffs' privacy interests before it terminates on November 29, 2015. Developments during the two years since this Court last addressed the special-needs analysis have substantially changed the relevant landscape and further reduced any potential for the program to meaningfully intrude on such interests.

First, any infringement on Plaintiffs' privacy interests attributable to NSA collection of bulk telephony metadata is diminished by its forthcoming termination. Congress has determined

[24] A court's application of the special-needs analysis is "not meant to transfer from politically accountable officials to the courts the decision as to which among reasonable" alternative "techniques should be employed to deal with a serious public danger," *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 453 (1990), because "the choice among . . . reasonable alternatives remains with the governmental officials who have a unique understanding of, and a responsibility for, limited public resources." *Id.* at 453-54.

that the Section 215 program will continue for only a matter of weeks, until November 29, before the targeted collection program is inaugurated. That is a profound change in the circumstances that led the Court to find a violation of Plaintiffs' privacy interests in the first place. *See Klayman*, 957 F. Supp. 2d at 32 (remarking that "there is the very real prospect that the program will go on for as long as America is combatting terrorism, which realistically could be forever!"). Indeed, the Second Circuit concluded under similar circumstances (then-imminent expiration of Section 215) that "[a]llowing the program to remain in place for a few weeks while Congress decides whether and under what conditions it should continue is a lesser intrusion on appellants' privacy than they faced at the time this litigation began." *ACLU*, 785 F.3d at 826. The imminent conclusion of the Section 215 program was thus sufficient reason for the court in *ACLU* to defer to the judgment of Congress and refrain from issuing a preliminary injunction, *see id*., and the same is true in the present case.

Second, the restrictions on review and dissemination of the metadata, which are written into the FISC's orders and already serve to lessen any intrusion, *see* Primary Order at 6-15; *see also Maryland v. King*, 133 S. Ct. 1958, 1979 (2013); *Earls*, 536 U.S. at 833, have been enhanced since the Court issued its December 2013 ruling. *See supra*, at 6. When this Court issued its initial decision, designated NSA officials were permitted to make the determination whether proposed selectors were reasonably suspected of association with identified foreign terrorist organizations, "without prior judicial approval of the investigative targets," Pls.' Br. at 22, *see also Klayman*, 957 F. Supp. 2d at 16. Today, FISC authorization is required for any selectors used to conduct queries that could reveal records of Plaintiffs' calls (or anyone else's) to NSA analysts, thus further diminishing the potential for unwarranted intrusions on their privacy interests. Also further minimizing the potential for infringement on Plaintiffs' privacy interests is the limitation on query results to metadata within two "hops," rather than three, of

suspected terrorist selectors. This limitation reduces the already de minimis odds that analysts' (judicially approved) queries will retrieve records of Plaintiffs' calls.

Indeed, with the possibility of the program continuing indefinitely now eliminated by the USA FREEDOM Act, as small as the odds were of metadata pertaining to Plaintiffs' calls ever being reviewed, the odds of that occurring *in the next two months* are now far smaller. Similarly, any infringement on Plaintiffs' privacy due to the NSA's accumulating another two months of bulk data is substantially mitigated by the fact that, after November 29, 2015, the NSA analysts will no longer be permitted to query that data for analytic purposes, whereas, had the program continued, it would have had analytic access to those data for up to the next five years.[25] At this stage, the program's potential for intrusion on Plaintiffs' privacy interests is minimal, and finite.

These developments—including greater judicial oversight of the Section 215 program, and its limited remaining duration—substantially mitigate any potential for intrusion upon Plaintiffs' privacy interests, and thus have altered the special-needs analysis in which the Court engaged two years ago. The reduced potential for infringement of Plaintiffs' privacy is far outweighed by the Government's interest in preserving its capacity to detect terrorist threats, in the midst of an evolving threat environment, until the targeted program of telephony metadata collection becomes fully operational. Continued operation of the Section 215 program for that purpose and that limited period of time, in accordance with the considered judgment of Congress, is therefore reasonable, and constitutional, under the special needs doctrine.

[25] Of course, under the principles of the Supreme Court's decisions in *Place*, *Jacobsen*, *Karo*, and other precedents, electronic queries of metadata collected by the NSA that do not expose records of Plaintiffs' calls to scrutiny by human analysts do not constitute intrusions on Plaintiffs' Fourth Amendment privacy interests at all. *See supra*, at 21-22. But even if it were otherwise, the fact that queries of the database are performed electronically and not manually at the very least "lessen[s] the intrusion." *ACLU*, 785 F.3d at 802.

III. THE BALANCE OF THE EQUITIES AND THE PUBLIC INTEREST—AS REFLECTED IN THE CONSIDERED JUDGMENT OF THE POLITICAL BRANCHES—WEIGH AGAINST AN INJUNCTION THAT WOULD DISRUPT THE TRANSITION TO THE TARGETED COLLECTION PROGRAM.

"[C]ourts of equity should pay particular regard for the public consequences in employing the extraordinary remedy of injunction," *Winter*, 555 U.S. at 24, in assessing whether any irreparable injury to plaintiffs "is outweighed by the public interest," *id.* at 23. Indeed, a "proper consideration of these factors *alone* [may] require a denial of the requested injunctive relief," even where plaintiffs have shown a likelihood of success on the merits and irreparable injury. *See id.* (emphasis added). In *Winter*, for example, the Supreme Court did not reach the lower courts' conclusions that the plaintiffs had demonstrated a "strong likelihood of prevailing on the merits" and irreparable harm "to a near certainty," *id.* at 21, because the Court concluded that the proposed injunction's "adverse impact on the public interest in national defense" foreclosed the relief sought. *See id.* at 24. Such consideration of the public interest is required—and may weigh against injunctive relief—even where the irreparable injury alleged is an infringement on constitutional rights. *See, e.g.*, *In re Navy Chaplaincy*, 697 F.3d 1171, 1179 (D.C. Cir. 2012); *Davis v. Billington*, 76 F. Supp. 3d 59, 68 (D.D.C. 2014).[26]

While a court's equitable discretion ordinarily allows it to consider "any and all factors that might relate to the public interest," that is not so "[o]nce Congress, exercising its delegated powers, has decided the order of priorities in a given area." *United States v. Oakland Cannabis Buyers' Coop.*, 532 U.S. 483, 497 (2001). Courts of equity must follow "the balance that

[26] In *Navy Chaplaincy*, plaintiffs pleading Establishment Clause violations were presumed to have shown irreparable harm, but the balance of equities and the public interest weighed against an injunction based on "the professional judgment of military authorities regarding the harm that would result to military interests if an injunction were granted." 697 F.3d at 1179. Likewise, the court in *Davis* declined to issue a preliminary injunction finding that, "[a]lthough a preliminary injunction would ensure that the First Amendment rights of federal government employees are not unnecessarily restricted, it could also . . . interfere with . . . the important mission of the Congressional Research Service." 76 F. Supp. 3d at 68.

Congress has struck in a statute." *id.* (quoting *TVA v. Hill*, 437 U.S. 153, 194-95 (1978)), and "cannot 'ignore the judgment of Congress, deliberately expressed in legislation,'" *id.* (quoting *Virginian Ry. Co. v. Sys. Fed'n No. 40*, 300 U.S. 515, 551 (1937)).[27]

Through the USA FREEDOM Act—the product of nearly two years of dialogue and debate between the political branches—Congress has balanced the equities at stake here; it has "gauge[d] changing public attitudes, . . . draw[n] detailed lines, and . . . balance[d] privacy and public safety in a comprehensive way," *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (observing that a "legislative body is well situated" to undertake such a task). And it has determined that the bulk telephony metadata program should end only after a brief transition period at which time the new targeted program can be brought online, *see supra*, at 10-11, reflecting its considered judgment that the public interest in maintaining the capabilities of this program on an interim basis to combat the evolving terrorist threat outweighs any short-term infringement on privacy interests. Under the Supreme Court's precedents, the Court should defer to that judgment.[28]

The evolving nature of the terrorist threat to the United States, its people, and U.S. interests abroad gives context to the political branches' determination. *See* Paarmann Decl. ¶¶ 5-12. Even more so than in 2013, the United States faces an "increasingly diffuse threat environment," *id.* ¶ 9, in which ISIL 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.* ¶¶ 6-8.

---

[27] *See also, e.g.*, *Brown v. Plata*, 131 S. Ct. 1910, 1944, 1946 (2011) (following the requirements of the Prison Litigation Reform Act in fashioning equitable remedies to address unconstitutional prison conditions).

[28] Of course Congress may not prioritize policy goals above the Constitution, *Gordon*, 721 F.3d at 652-53, here the political branches have weighed the public interest in national security and privacy, as Justice Alito instructed in *Jones*, 132 S. Ct. at 964 (Alito, J., concurring), and fashioned, in the USA FREEDOM Act, a solution that comports with established Fourth Amendment jurisprudence, *see supra*, at 32-37. Under *Oaklan Cannabis*, this policy determination regarding how best to end the program should be dispositive.

Telephony metadata analysis can provide information earlier than other investigative methods, and act as an "early warning system" of potential threats against the Nation's security. *Id.* ¶ 12. 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 each of those sources can be considered together to compile as complete a picture as possible of a potential terrorist threat." *Id.* ¶ 10. "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.*

In this environment, the value of the Section 215 program's capabilities cannot be discounted—the sooner, for example, that the FBI obtains information about particular threats to the national security, the more likely the Bureau will be able to prevent and protect against them. *Id.* ¶ 12. As noted, courts have long recognized that "attempts to counter foreign threats to the national security require the utmost . . . speed." *Truong Dinh Hung*, 629 F.2d at 913; *see also, e.g.*, *In re Directives*, 551 F.3d 1004, 1011 (FISC. Ct. Rev. 2008) (recognizing "a high degree of probability" that a "hind[rance]" to "the [G]overnment's ability to collect time-sensitive information . . . would impede . . . vital national security interests").[29] Especially in light of the increased risk of small-scale attacks, earlier receipt of information may advance an FBI investigation and contribute to the disruption of a terrorist attack that, absent the metadata tip, the FBI might not have prevented in time. *Id.* ¶ 12. In this context, speed matters.

[29] Congress acted in express recognition of the time-sensitivity of counter-terrorism intelligence when it enacted section 702 of FISA, 50 U.S.C. § 1881a, to enhance the Government's intelligence-collection authority. *See, e.g.*, H.R. Rep. No. 112-645(II), 112th Cong., 2d Sess., at 2 (Aug. 2, 2012) (highlighting "speed and agility necessary to meaningfully collect foreign intelligence"); S. Rep. No. 112-174, 112th Cong., 2d Sess., at 2 (June 7, 2012) (emphasizing importance of the Intelligence Community's "ability . . . to respond quickly to new threats and intelligence opportunities"). *See also Amnesty Int'l*, 133 S. Ct. at 1144.

The specific effects upon the Section 215 program, and attendant risk of harm to national security that may flow from any preliminary injunction issued in this matter, would, of course, be shaped by the contours of any such order. *See* Potter Decl. ¶¶ 20-27. The preliminary injunction granted in the Court's December 16, 2013 Order, if not stayed pending appeal, would have 1) barred the Government from collecting, as part of the Section 215 program, any telephony metadata associated with Plaintiffs Klayman's and Strange's calls; and 2) required the Government to destroy such data if any were previously collected under the program. *Klayman.* 957 F. Supp. 2d at 36. Following the Court's Order, the Government engaged in extensive inter-agency discussions and planning regarding the steps required to comply should the injunction have been upheld on appeal. *See* Potter Decl. ¶ 20. The NSA's examination of the steps necessary to implement the previously-issued injunction revealed that any injunction requiring *immediate* cessation of collection of or analytic access to data associated with Plaintiffs' telephone calls (if any) would necessitate a termination of all collection and queries of metadata already collected under the program. *See id.* ¶¶ 22-23, 25-27. This is so for several reasons.[30]

First, two steps that must precede the implementation of such an injunction are not within the NSA's control. *See id.* ¶¶ 22-23. As a preliminary matter, as this Court has noted, *see* 957 F. Supp. 2d at 36, n.70, the NSA would need to be provided (at a minimum) with the telephone numbers or calling card numbers used by the Plaintiffs and the dates of usage of those telephone numbers or calling card numbers, Potter Decl. ¶ 22, because the call-detail records collected under the program include dialing and receiving telephone numbers (among other

[30] As Plaintiffs now seek the preservation of any such data, rather than its destruction, *see* Proposed Order, Pls.' Mot., the discussion herein of the potential effects on the program of a preliminary injunction does not address in detail the difficulty of complying with an order (if any) to destroy such records. However, an order requiring the destruction of metadata associated only with Plaintiffs' or any particular individuals' calls (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. Potter Decl. ¶ 21.

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 id.* (citing Aug. 27, 2015 Primary Order at 3, n.1). Thus, compliance with any injunction concerning the telephony metadata associated with Plaintiffs' calls would first require that Plaintiffs: (1) provide the NSA 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 NSA with timely updates to this information when new numbers are used or when Plaintiffs cease to use certain numbers. *Id.* Until Plaintiffs provide this information, the only way the NSA could ensure compliance with an injunction barring collection or queries of telephony metadata associated with Plaintiffs' calls would be to terminate all collection and querying under the program altogether. *Id.*

Second, after receiving the Plaintiffs' telephone numbers, the NSA would need to engage with the FISC regarding the implementation of any preliminary injunction. *Id.* ¶ 23. This would be necessary because the FISC's August 27, 2015 Primary Order restricts searches of the metadata to queries undertaken for purposes of obtaining foreign intelligence information (using FISC-approved selectors) and for limited technical purposes, such as making the data usable for intelligence analysis. *Id.* at (discussing Aug. 27, 20 15 Primary Order at 5-9).[31]

Thus, if this Court were to issue an injunction requiring the NSA to take action regarding 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. *Id.* The NSA cannot estimate the amount of time necessary to complete this process, since the timeframe would depend upon the

[31] That Order provides: "[t]he Government is . . . prohibited from accessing BR metadata for any purpose except as described [there]in." Potter Decl. ¶ 23. (quoting Aug. 27, 2015 Primary Order at 4).

FISC's response to the Government's proposal, including whether it would require the Government to seek a modification of its Orders to perform such queries. *Id.* Thus, if the NSA were required to comply immediately with an injunction as described above, without having first engaged with the FISC and, if deemed necessary, having obtained a modification of the FISC's Orders to permit the NSA to query the metadata using the Plaintiffs' telephone numbers, compliance would require termination of all collection and queries of data already collected under the program. *Id.*

Even after completion of these preliminary steps, an injunction requiring immediate cessation of collection of and access to records of Plaintiffs' calls would necessitate termination of all collection and analytic access to all data previously collected under the program until the technical means of compliance could be developed and/or implemented. *See id.* ¶¶ 25-27. If an injunction barring collection of metadata pertaining to Plaintiffs' calls were intended to prohibit the NSA from receiving such data from providers in the first instance, the NSA would need to rely upon participating providers to develop the capability to filter out records containing specific identifiers from their bulk productions before they were transmitted to the NSA. *Id.* ¶ 25. Because, by technical necessity, such work would be done by the providers, it is not possible for the NSA to estimate the length of time (or amount of funding) needed to develop this capability. *Id.* In the meantime, however, to ensure compliance with the Court's injunction all collection of telephony metadata under the program would have to cease. *Id.*

If an injunction barring collection instead permitted the NSA to filter out records associated with Plaintiffs' calls, if any, after receipt, it would be possible, as a technical matter, for NSA to develop a process to delete or segregate upon ingestion into its databases any call detail records (if any) containing the selectors identified by Plaintiffs. *Id.* ¶ 26. NSA estimates, however, that it would require two full-time employees working approximately two months to

design, code, and test such a process. *Id.* In light of that timeframe, it is unlikely that this capability could become operational before the termination of the program, and the start date of the new targeted collection program on November 29, 2015. *Id.* [32]

Finally, with respect to a potential injunction requiring the NSA to discontinue analytic access to any records about Plaintiffs' calls (if any) that may already have been collected under the program, NSA technical personnel estimate such a process could be completed within about two weeks *after* the receipt of Plaintiffs' telephone numbers and the time-frames during which they were used. *Id.* ¶ 27.[33] Unless and until that process is completed, however, to ensure compliance with an injunction requiring immediate cessation of analytic access to records of Plaintiffs' calls (if any) would require the suspension of all queries of the database. *Id.*

Thus, the consequences for the Government and the public interest in national security of injunctive relief granted here would vary, depending on the injunction's specific requirements. The impact could range from the diversion of personnel and financial resources from other NSA intelligence programs, to the termination in whole or in part of the Section 215 program—in the face of an increasingly perilous threat environment, and in contravention of the will of Congress—before the targeted program of collection will be ready to fill the intelligence gap left behind.

While an injunction could create the very intelligence gap that Congress sought to avoid, in the current threat environment, by enacting the USA FREEDOM Act, any harm to Plaintiffs' privacy interests attributable to the NSA's bulk collection of telephony metadata is, as discussed above, diminished by the program's approaching conclusion. Whether records about Plaintiffs'

[32] Adding other personnel to the project would have only a marginal effect on shortening the time needed to complete this process. Potter Decl. ¶ 26 n.2.

[33] The NSA has already developed a process that can be used to prevent analytic access to metadata containing specified identifiers. Potter Decl. ¶ 27. 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. *Id.*

telephone calls are collected in the first instance, is speculative. *See supra*, at 16-19. Even if the Court were to find otherwise, Plaintiffs have presented no basis on which to conclude that records about their calls would be retrieved by analysts conducting FISC-approved queries within the next two months, after which analytic access to the bulk metadata collected before November 29 will terminate altogether. Indeed, as of that date—less than two months from now—Plaintiffs' request for prospective injunctive relief will be rendered moot,[34] yet another circumstance that plainly weighs against further equitable relief.

Moreover, even if the Court concluded that records about Plaintiffs' calls are being or have been collected as part of this program, the harm to Plaintiffs would be no greater than in *ACLU*, where the Second Circuit, emphasizing that Section 215 (at the time) was expiring on its own terms in several weeks, declined to issue a preliminary injunction notwithstanding that the plaintiffs alleged a deprivation of constitutional rights. 785 F.3d at 825–26. The court in *ACLU* highlighted that it was "[a]llowing the Program to remain in place for a few weeks"—in light of the Government's representations "that the program is necessary for maintaining [the] national security"—to permit Congress to "decide[] whether and under what conditions [the Program] should continue." *Id.* at 826. Here, after years of deliberation and debate, Congress has done just that; it has balanced the equities and determined that the brief transition authority provided by the USA FREEDOM Act is in the public interest in the current threat environment. The minimal, speculative, and temporary harm to Plaintiffs' privacy should not—and, indeed, under *Oakland Cannabis Buyers' Coop*, cannot—justify depriving the public of that protection.

CONCLUSION

Plaintiffs' renewed motion for a preliminary injunction should be denied.

[34] *See, e.g.*, *Log Cabin Republicans* v. *United States*, 658 F.3d 1162, 1166-67 (9th Cir. 2011) (per curiam); *see also, e.g.*, *Burke* v. *Barnes*, 479 U.S. 361, 363-64 (1987); *U.S. Dep't of the Treasury v. Galioto*, 477 U.S 556, 559-60 (1986).

Dated: October 1, 2015

Respectfully submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

/s/ James J. Gilligan
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 6102
Washington, D.C. 20044
Phone: (202) 514-3358
Fax: (202) 616-8470
james.gilligan@usdoj.gov

Counsel for Government Defendants