UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

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

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

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

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

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and did not issue its decision until August 28, 2015—nearly three months *after* the USA PATRIOT Act had lapsed and had been replaced by the USA FREEDOM Act, which was enacted on June 2, 2015.

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

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

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

---

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

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

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

BACKGROUND

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

A. Statutory Framework

1. The Section 215 Bulk Telephony Metadata Program

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

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

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

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

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

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

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

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

2. The USA FREEDOM Act

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

---

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

Program with one that would "give the public greater confidence that their privacy is appropriately protected," while maintaining the intelligence tools needed "to keep us safe." President Barack Obama, Statement by the President on the Section 215 Bulk Metadata Program (Mar. 27, 2014), http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program. In response to this directive, Congress ultimately enacted the USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015) ("USA FREEDOM Act"), on June 2, 2015. Relevant to this Opinion, the USA FREEDOM Act expressly prohibits the Government from obtaining telephony metadata in bulk, but not until November 29, 2015. USA FREEDOM Act §§ 103, 109; *see* Potter Decl. ¶ 11. It seems that the NSA requested this 180-day delay to allow time to transition from the Bulk Telephony Metadata Program to a new replacement program Congress conceived—a model whereby targeted queries will be carried out against metadata held by telecommunications service providers and the resulting data subsequently produced to the Government. *See id.* § 101. As the Government has explained, this 180-day transition period will avoid a so-called "intelligence gap" that would follow if the current Program terminated before the new targeted metadata querying program is fully operational. Gov't's Opp'n 34; *see* 161 Cong. Rec. S3275 (daily ed. May 22, 2015) (statement of Sen. Leahy) (having printed in the record a letter from the NSA which stated: "NSA assesses that the transition of the program to a query at the provider model is achievable within 180 days, with provider cooperation. . . . [W]e will work with the companies that are expected to be subject to Orders under the law by providing them the technical details, guidance, and

compensation to create a fully operational query at the provider model."). To date, however, the Government has failed to identify any concrete consequences that would likely result from this so-called "intelligence gap." And while Congress refrained for obvious political reasons from expressly authorizing a six-month extension of the Bulk Telephony Metadata Program,[5] the Government conveniently went immediately thereafter to the FISC to seek judicial authorization to continue the Program during the transition period, consistent with its prior authorization under the USA PATRIOT Act. *See* Mem. of Law 5, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, No. BR 15-75 (FISC June 2, 2015). Not surprisingly, the FISC agreed. *See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, No. BR 15-75 (FISC June 29, 2015). As such, during the current 180-day transition period, the Bulk Telephony Metadata Program has continued by judicial, not legislative, fiat.[6]

B. Procedural Posture

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

---

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

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

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

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

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

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

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

---

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

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

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

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

ANALYSIS

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

---

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

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

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

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

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

---

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

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

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

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

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

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

No principle is more fundamental to the balance of federal power than the "constitutional limitation of federal-court jurisdiction to actual cases or controversies." *DaimlerChrysler Corp v. Cuno*, 547 U.S. 332, 341 (2006) (internal quotation marks omitted). Inherent in this principle is the requirement that each plaintiff demonstrate adequate standing to press their claims in federal court. *Raines v. Byrd*, 521 U.S. 811, 818 (1997). "To establish Article III standing, an injury must be 'concrete,

---

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

i. Nature of the Privacy Interest

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

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

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

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

ii. Character and Degree of Governmental Intrusion

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

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

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

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

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

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

---

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

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

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

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

iii. Nature of Government's Interest and Efficacy

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

---

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

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

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

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

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

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

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

B. Plaintiffs Will Suffer Irreparable Harm Absent Injunctive Relief.

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

CONCLUSION

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

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

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

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

RICHARD J. LEON
United States District Judge

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