UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs,

v.

JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; CHARLES T. HAGEL, in his official capacity as Secretary of Defense; ERIC H. HOLDER, in his official capacity as Attorney General of the United States; and ROBERT S. MUELLER III, in his official capacity as Director of the Federal Bureau of Investigation,

Defendants.

13 Civ. 3994 (WHP)

ECF Case

DEFENDANTS' MEMORANDUM OF LAW IN OPPOSITION TO PLAINTIFFS' MOTION FOR A PRELIMINARY INJUNCTION

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director

ANTHONY J. COPPOLINO
Deputy Director

JAMES J. GILLIGAN
Special Litigation Counsel

MARCIA BERMAN
Senior Trial Counsel

BRYAN DEARINGER
Trial Attorney
U.S. Department of Justice
Washington, D.C.

PREET BHARARA
United States Attorney for
the Southern District of New York

DAVID S. JONES
TARA M. La MORTE
JOHN D. CLOPPER
CHRISTOPHER HARWOOD
Assistant United States Attorneys
86 Chambers Street, 3rd Floor
New York, NY 10007
Tel. No. (212) 637-2739 (Jones)
Fax No. (212) 637-2730
david.jones6@usdoj.gov
tara.lamorte2@usdoj.gov
john.clopper@usdoj.gov
christopher.harwood@usdoj.gov

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES AND REGULATIONS

MISCELLANEOUS

PRELIMINARY STATEMENT

Plaintiffs challenge a program by which the National Security Agency (NSA) obtains, pursuant to orders of the Foreign Intelligence Surveillance Court (FISC), bulk telephony metadata – business records created by telecommunications service providers that include such information as the telephone numbers placing and receiving calls, and the time and duration of those calls. Targeted electronic searches of these data, based on telephone numbers or other identifiers associated with foreign terrorist organizations, can reveal communications between known or suspected terrorists and previously unknown terrorist operatives, located in this country, who may be planning attacks on U.S. soil. Information gleaned from analysis of bulk telephony metadata obtained under this program has made important contributions to the FBI's counter-terrorism mission. The bulk collection of telephony metadata for these limited purposes has been authorized and periodically reauthorized over the past seven years under thirty-four separate orders issued by fourteen separate judges of the FISC. The program operates under FISC orders, together with stringent supervision and oversight by all three branches of Government, to prevent access to, use, or dissemination of the data for any purpose other than foreign intelligence. In a detailed opinion issued on August 29, 2013 (Exhibit A, hereto), the FISC concluded that the telephony metadata program is authorized by statute, and lawful under the Constitution.

Plaintiffs' motion for a preliminary injunction is based entirely on conjecture as to how the Government might misuse telephony metadata collected under the program, and consequences that might ensue. While Plaintiffs purport to base their case on public statements by the Government about how this program operates, they ignore crucial limitations, described in the very same documents, on the Government's collection and use of the metadata, and contend,

with no basis in fact, that the Government is using these metadata to track the associations of U.S. citizens, compile profiles on them, and draw comprehensive social maps of their lives.

Plaintiffs' portrayal of the program is unsupported by any evidence. Under the challenged program, the NSA collects only numeric telephony metadata – *i.e.*, call detail records – including such session-identifying information as the telephone numbers that placed and received a call, and the date, time, and duration of the call. The Government does not collect the substantive content of any telephone call under this program, it does not listen to or record the contents of any call, nor does it collect cell-site location information. In addition, under this program the Government does not collect the name, address, or financial information of any subscriber, customer, or any party to a call. The metadata collected under this program do not reveal that a whistleblower called the ACLU, or that an individual called an abortion clinic, a criminal-defense lawyer, or a suicide hotline, as Plaintiffs speculate.

Equally important, the FISC orders authorizing the program prevent the NSA from accessing the metadata collected under the program to ascertain any such information or to draw "comprehensive social maps" of anyone's lives. The NSA may only query the collected metadata for counter-terrorism purposes, and even then, only if there is a reasonable, articulable suspicion that the selection term (e.g., the telephone number) to be queried is associated with a specified foreign terrorist organization approved for targeting by the FISC. This requirement bars the type of indiscriminate querying of the metadata, using identifiers not connected with terrorist activity, about which Plaintiffs speculate. As a result, only a tiny fraction of the collected metadata are ever reviewed, much less disseminated, by NSA analysts. These constraints on the NSA's access to and use of the metadata are critical to the program's continued authorization by the FISC, and the FISC has not hesitated to take action to enforce them.

The errors in Plaintiffs' characterization of the program undercut their motion for a preliminary injunction, first belying their assertions of irreparable injury. Both the claim that the Government has intruded on Plaintiffs' sensitive associations and communications, and that whistleblowers, clients, and others may be chilled from contacting Plaintiffs as a result, are based entirely on speculation for which no proof is offered. Injury so speculative as Plaintiffs assert is insufficient to establish the irreparable harm required for a preliminary injunction, or, for that matter, the injury-in-fact required to demonstrate their standing to sue.

Plaintiffs' misconceptions about the telephony metadata program also negate any likelihood of success on the merits of their claims. The Supreme Court squarely held in *Smith v. Maryland*, 442 U.S. 735 (1979), that there is no reasonable expectation of privacy in non-content information such as the numbers dialed on a telephone, and that is all that is at issue here. Thus, there has been no search for purposes of the Fourth Amendment. Plaintiffs' First Amendment claim also rests entirely on their hypothetical premise that the program tracks all of their sensitive contacts with members, clients, whistleblowers, and others with whom they collaborate in their work to government scrutiny. But no parallel can be drawn between the collection of dialed telephone numbers and other telephony metadata, and circumstances in which individuals or organizations were compelled to disclose personally identifying information, or membership lists, based on their protected associational activities.

Plaintiffs' statutory claim that the telephony metadata program exceeds the Government's authority under the Foreign Intelligence Surveillance Act (FISA) is also unlikely to succeed on the merits. As an initial matter, judicial review of this claim is implicitly precluded by statute, as set forth in Defendants' motion to dismiss. Plaintiffs' statutory argument also fails to grapple with the fact that fourteen separate judges of the FISC have concluded on thirty-four occasions that the Government demonstrated, as the statute requires, reasonable grounds to believe that the

telephony metadata as a whole are indeed relevant to authorized investigations to protect against international terrorism. The FISC fully appreciated that most of the metadata records collected are unrelated to terrorist activity, but it also recognized that the bulk collection of telephony metadata is important to the Government's counter-terrorism efforts because it creates a comprehensive, historical repository that permits NSA to undertake a retrospective analysis of terrorist-related communications and potentially to identify unknown terrorist operatives that might otherwise go undetected. Contrary to Plaintiffs' contentions, this type of analysis cannot be as effectively performed using traditional, targeted intelligence-gathering capabilities.

In sum, the Section 215 telephony metadata program is an important tool in the Government's counter-terrorism arsenal, and it is lawful. Conjecture about how the program might be abused, without regard to the safeguards against such abuse, and without evidence that Plaintiffs have suffered irreparable injury, does not justify the extraordinary remedy of preliminary injunctive relief. Plaintiffs' motion for a preliminary injunction should be denied.

BACKGROUND[1]

One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. The exploitation of terrorist communications is a critical tool in this effort, and analysis of bulk telephony metadata provides the Government with a timely and effective means of discovering communications with and among unknown terrorist operatives. Declaration of Teresa H. Shea, Signals Intelligence Director, NSA ("Shea Decl.") ¶¶ 6-8; Declaration of R.J. Holley, Acting

[1] We respectfully refer the Court to Defendants' Motion to Dismiss (ECF No. 33) for a discussion of the relevant statutory background and Plaintiffs' allegations, focusing here instead on details of the telephony metadata program that are not included in the Complaint, and so could not be addressed in Defendants' motion.

Assistant Director, Counterterrorism Division, FBI ("Holley Decl.") ¶¶ 4-5, 8 (both filed herewith).

Indeed, the telephony metadata program is aimed at filling a significant intelligence gap identified by the September 11, 2001 attacks. Prior to that tragic event, the NSA intercepted and transcribed seven calls made by hijacker Khalid al-Mihdhar, who was living in San Diego, California, to a telephone identifier associated with an al Qaeda safe house in Yemen. The NSA intercepted these calls using overseas signal intelligence capabilities, but those capabilities did not capture the calling party's telephone number identifier. Because they lacked the U.S. telephone identifier, NSA analysts mistakenly concluded that al-Mihdhar was overseas. Telephony metadata, however, if available at the time, would have included the missing information and might have permitted NSA analysts to place al-Mihdhar within the United States prior to the attacks and advise the FBI of that information. Shea Decl. ¶ 11.

Plaintiffs attempt to depict the telephony metadata program as one in which Americans' communications are "track[ed]" by intelligence officials and used to compile "rich profiles" and "comprehensive social maps" of their lives, but that description bears no resemblance to this stringently controlled program. Under the program, the Government obtains orders from the FISC, pursuant to FISA's "business records" provision, 50 U.S.C. § 1861, enacted by section 215 of the USA-PATRIOT Act, Pub. L. 107-56, 115 Stat. 272 (Section 215), that direct certain telecommunications service providers to produce telephony metadata, also referred to as call detail records, to the NSA. The NSA then stores, queries, and analyzes the metadata for counter-terrorism purposes. Under the terms of the FISC's orders, the Government's authority to continue the program expires after 90 days and must be renewed. The FISC first authorized the program in May 2006, and since then it has renewed the program thirty-three times under orders issued by fourteen different FISC judges. Shea Decl. ¶¶ 13-14, 16-17, 20; Holley Decl. ¶¶ 3, 6.

Under the FISC's orders, the NSA is authorized to collect, as to each call, the telephone numbers that placed and received the call, other session-identifying information (*e.g.*, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card number, and the date, time, and duration of a call. The data are numerical only. The FISC's orders authorizing this program do not allow the NSA to collect the substantive content of any telephone call, nor the name, address, or financial information of a subscriber, customer, or any party to a call. The Government cannot, under this program, listen to or record the contents of anyone's communications. Shea Decl. ¶¶ 13, 15, 18; Holley Decl. ¶¶ 5, 7, 11.

The Government obtains these FISC orders by submitting detailed applications from the FBI explaining that the records are sought for investigations to protect against international terrorism that concern specified foreign terrorist organizations identified in the application. Holley Decl. ¶ 10. As required by Section 215, the application contains a statement of facts showing that there are reasonable grounds to believe that the metadata as a whole are relevant to the investigations of these organizations. The application is supported by a declaration from a senior official of NSA's Signals Intelligence Directorate. *Id.*

The FISC's orders strictly limit access to, analysis of, and dissemination of information derived from the metadata to valid counter-terrorism purposes. Primary Order at 4-17 (Shea Decl. Exh A); Holley Decl. ¶ 8. The NSA may access the metadata for purposes of obtaining foreign intelligence information only through "contact-chaining" queries (term searches) of the metadata using identifiers (typically telephone numbers) approved as "seeds" by one of twenty-two designated officials in NSA's Signals Intelligence Directorate. Such approval may only be given upon a determination by one of these officials that, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts

giving rise to a reasonable, articulable suspicion that the selection term to be queried is associated with one or more of the specified foreign terrorist organizations. Where the selection term is reasonably believed to be used by a U.S. person, NSA's Office of General Counsel must also determine that the term is not regarded as associated with a foreign terrorist group solely on the basis of activities protected by the First Amendment. These determinations are effective for a finite period of time. Shea Decl. ¶¶ 19-23, 31. This "reasonable, articulable suspicion" requirement bars the indiscriminate querying of the telephony metadata based on identifiers not connected with terrorist activity. Indeed, because of this requirement, the vast majority of the data obtained under this program are never seen by any person; only the tiny fraction of the records responsive to queries authorized under the "reasonable, articulable suspicion" standard are reviewed or disseminated by NSA analysts. *Id.* ¶¶ 20, 23.[2]

Also under the FISC's orders, once the NSA has obtained approval to conduct a query, the results are limited to records of communications within three "hops" from the seed. That is, the query results may only include identifiers and associated metadata having a direct contact with the seed (the first "hop"), identifiers and associated metadata having a direct contact with first "hop" identifiers (the second "hop"), and identifiers and associated metadata having a direct contact with second "hop" identifiers (the third "hop"). *Id.* ¶¶ 22, 31. Query results do not

[2] The attached NSA declaration addresses in detail other "minimization procedures" contained in the FISC orders, for minimizing the retention of metadata and the dissemination of U.S.-person information derived from the metadata, including a rigorous series of procedural, technological, and legal controls, intensive internal and external oversight, and reporting requirements to Congress and the FISC. Shea Decl. ¶¶ 29-35; *see* Primary Order at 4-17.

include the names or addresses of individuals associated with the responsive telephone numbers, because that information is not included in the database in the first place. *Id.* ¶ 21.[3]

The ability under this program to accumulate metadata in bulk, and to quickly conduct contact-chaining analyses beyond the first hop, is crucial to the utility of the database. These capabilities allow use of the database to conduct a level of historical analysis, and the discovery of contact links, that cannot practically be accomplished through targeted intelligence-gathering authorities, such as acquiring metadata of only direct communications with known terrorist operatives, or prospectively acquiring the metadata of communications occurring after a pen-register/trap-and-trace (PR/TT) device is installed. For example, the metadata may reveal that a seed telephone number has been in contact with a previously unknown U.S. telephone number. Examining the chain of communications out to the second and in some cases a third hop may reveal a contact with other telephone numbers already known to be associated with a foreign terrorist organization, thus establishing that the previously unknown telephone number is itself likely associated with terrorism. This type of contact-chaining under the program is possible because the bulk collection of telephony metadata creates an historical repository that permits retrospective analysis of terrorist-related communications across multiple telecommunications networks, and that can be immediately accessed as new terrorist-associated telephone identifiers come to light. *Id.* ¶¶ 46-49, 57-63; Holley Decl. ¶¶ 27-29.

Not only is NSA's access to the telephony metadata obtained under this program limited as described above, its dissemination of query results is also tailored to provide only the most

[3] Based on an entirely hypothetical assumption that each individual communicates with forty other persons, Plaintiffs estimate that a query of a single individual's telephone number would capture metadata records concerning the calls of more than two million people. Pls.' PI Br. at 7. There is, however, no "typical" number of records responsive to a given query – the number varies widely – and Plaintiffs' hypothetical estimate is erroneous, in any case, as a matter of simple math. The correct number of records, using Plaintiffs' hypothetical example of forty contacts per person, would be 65,640, not over two million. Shea Decl. ¶ 25 & n.1.

useful foreign intelligence information to the FBI and other agencies. The NSA does not use queries of these data to provide the FBI with profiles on suspected terrorists or comprehensive records of their associations. Nor does it provide the FBI with a list of all identifiers directly or indirectly connected (at one, two, and three hops) with a suspected terrorist identifier. Such a "data dump" of contact information would be of little investigative value to the FBI, particularly in the midst of investigations where time may be of the essence. Rather, the NSA applies the tools of signals intelligence tradecraft to focus only on those identifiers which, based on the NSA's analytic judgment and experience, and other intelligence available to it, may be of use to the FBI in detecting persons in the United States who may be associated with the specified foreign terrorist organizations, and acting in furtherance of their goals. Shea Decl. ¶¶ 26, 28. Prior to dissemination of any U.S.-person information outside NSA, a senior NSA official must determine that the information is in fact related to counter-terrorism information, and is necessary to understand that information or assess its importance. Primary Order at 13; Shea Decl. ¶ 32. And the NSA may not provide the FBI with any information derived from the metadata unless it is responsive to query terms approved under the "reasonable, articulable suspicion" standard. Shea Decl. ¶ 23.[4]

The Government has recently made public FISC orders and opinions concerning various failures to fully implement and comply with these minimization procedures, 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

[4] Plaintiffs may cite a recent article in the New York Times claiming that the NSA has been utilizing collections of data to "create sophisticated graphs of some Americans' social connections." James Risen & Laura Poitras, *NSA Gathers Data on Social Connections of U.S. Citizens*, N.Y. Times, Sept. 28, 2013. Even assuming the truth of this article for the sake of argument, which the Government neither confirms nor denies, the article makes clear that metadata collected under authority of Section 215 are not used in this alleged activity. *Id.*

suspending the Government's authority to query the database without the court's approval) reauthorized the program in its current form. Importantly, even the most serious of these incidents did not involve the compilation of detailed profiles of Americans' lives, as Plaintiffs insinuate has been occurring.[5] Shea Decl. ¶¶ 36-43.

The telephony metadata program has contributed to the fight against terrorism in important ways. Metadata analysis provides information that assists the FBI in detecting, preventing, and protecting against terrorist threats to the national security of the United States by providing the predication to open investigations, advance pending investigations, and revitalize stalled investigations. It can also rule out avenues of investigation, allowing the FBI to redirect scare resources. Metadata analysis can also provide early warning signals that alert the FBI to individuals who are inside the United States and are linked to persons who pose a threat to the national security. Similarly, metadata analysis can be of importance in situations where timely information about communications by and among suspected terrorists may be necessary to prevent the occurrence (or recurrence) of terrorist attacks. Holley Decl. ¶¶ 8-9, 18-23, 28.

The accompanying FBI declaration discusses unclassified examples in which telephony metadata analysis, together with other intelligence methods, played a role in the FBI's counter-terrorism successes. *Id.* ¶¶ 24-26. One such example is the contribution of telephony metadata analysis to the FBI's disruption, in fall 2009, of the plan by al-Qa'ida associated terrorist

[5] The most serious compliance problem involved an "alert list" process by which telephone identifiers that had been associated with foreign terrorist organizations, but which in many cases had not been approved under the "reasonable, articulable suspicion" standard, were used, not as terms to query the metadata archive, but to alert analysts if identifiers associated with foreign terrorist groups were in contact with someone in the United States. Analysts could not query the database using these "alert list" identifiers to learn what numbers they had been in contact with unless and until they were approved under the "reasonable, articulable suspicion" standard. Shea Decl. ¶ 37. (Other compliance incidents have occurred since 2009, due to human error and technology issues, although not on the same scale as the incidents discovered in 2009. All have likewise been reported to the FISC and appropriately remedied.)

Najibullah Zazi and his associates to bomb the New York City subway. After signals intelligence, together with FBI investigative efforts, revealed that Zazi was in contact with al Qa'ida-associated terrorists, NSA received Zazi's telephone number from the FBI and ran it against the telephony metadata, identifying and passing additional leads back to the FBI for investigation. One of these leads revealed a previously unknown number for co-conspirator Adis Medunjanin, and corroborated his connection to Zazi as well as to other U.S.-based extremists. Ultimately, Zazi and his co-conspirators were arrested; Zazi pled guilty to conspiring to bomb the New York City subway system, and Medunjanin was sentenced to life in prison. *Id.* ¶ 26.

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) (quotation marks and citations omitted). 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). "[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); *see Salinger v. Colting*, 607 F.3d 68, 79-80 (2d Cir. 2010). Where, as here, the moving parties seek a mandatory injunction that alters the status quo, and that will affect government action taken in the public interest pursuant to a statutory scheme, the movants must make an even more compelling demonstration of entitlement to preliminary relief than is normally required. *Cacchillo v. Insmed, Inc.*, 638 F.3d 401, 406 (2d Cir. 2011); *see also Sussman v. Crawford*, 488 F.3d 136, 140 (2d Cir. 2007).

Further, a preliminary injunction cannot issue on the mere basis of speculation or possibility. *Winter*, 555 U.S. at 21-22. Rather than allowing relief based on a "'possibility' of

irreparable harm," *id.* at 21, the Supreme Court has emphasized that a preliminary injunction should issue only upon a showing that irreparable harm is "likely in the absence of an injunction." *Id.* at 22; *see also Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 118 (2d Cir. 2009). Moreover, 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.*

POINT I: PLAINTIFFS' ASSERTED INJURIES ARE TOO SPECULATIVE TO ESTABLISH THEIR STANDING, OR SHOW IRREPARABLE HARM

Plaintiffs have not shown that the injuries they claim to fear as a consequence of the telephony metadata program are real and immediate, as opposed to entirely speculative. This failure has two consequences: (1) Plaintiffs cannot meet the requirement of demonstrating a clear or substantial likelihood of success on their claims because they have not established their standing to pursue those claims; and (2) for essentially the same reasons, they cannot demonstrate that irreparable harm is likely absent an injunction.

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

Plaintiffs' request for a preliminary injunction must be denied because they have failed to establish their Article III standing. *Munaf*, 553 U.S. at 680. When a preliminary injunction is sought, a plaintiff may no longer rest on mere allegations in the complaint to establish standing, but must set forth by affidavit or other evidence "specific facts" establishing each element of standing, including that they have suffered, or imminently will suffer, an injury in fact. *See Cacchillo*, 638 F.3d at 404.

Plaintiffs have failed to set forth any evidence that the injury they assert is sufficiently real and immediate to satisfy Article III's standards. Plaintiffs' assertions of the consequences

they will suffer as a result of the telephony metadata program depend on speculation about how the Government might use metadata related to their calls, and that third-parties—such as current or prospective clients, or whistleblowers desiring their advice—might be "chilled" from contacting Plaintiffs because of the Government's use of the metadata, as they characterize it.

Plaintiffs allege that the Government uses metadata obtained under the challenged program to keep track of when and with whom Americans communicate, and to obtain "a rich profile of every citizen as well as a comprehensive record of citizens' associations with one another." Pls.' PI Br. at 1. Plaintiffs cite no evidence for these assertions, however, and the restrictions imposed on the program by the FISC's orders demonstrate the contrary. The NSA collects only telephone numbers and other metadata, without any information about to whom the phone numbers belong, and thus the metadata do not reveal whether a particular phone number called is, for example, an abortion clinic, ex-girlfriend, criminal-defense lawyer, or suicide hotline. Not only is there no subscriber-identifying information in the database, the FISC's orders only allow the database to be searched and records reviewed for counter-terrorism purposes, not to track or profile the activities and associations of average Americans. As a result, very few of the records are ever seen by any person, and it is speculation to suggest that metadata records of calls to or from Plaintiffs either have been or ever will be retrieved or reviewed through queries of the database. Shea Decl. ¶¶ 5, 15, 17, 19-23. Such speculation cannot substitute for the required demonstration that the "threatened injur[ies] [are] certainly impending." *Amnesty Int'l USA v. Clapper*, 133 S. Ct. 1138, 1147 (2013).

Nor have Plaintiffs advanced any evidence supporting their conjecture that third parties, fearing the Government can or will use call detail records to identify individuals with whom Plaintiffs speak, will refrain from calling them. The evidence they have submitted to support that proposition is uniformly speculative. *See, e.g.*, German Decl. ¶ 30 (speculating that "some

individuals may decide not to seek advice from me or the ACLU" based on their knowledge of the telephony metadata program); Shapiro Decl. ¶ 8 (opining that "there is a genuine risk that people who would otherwise speak on the telephone with the ACLU will refrain from doing so if they believe that the government will be able to learn that they have been communicating with us"). Standing, however, cannot be based on a "speculative chain of possibilities," *Amnesty Int'l*, 133 S. Ct. at 1150, including conjecture about third parties' reactions to hypothetical future events, *id*. at 1152 n.7. Plaintiffs accordingly have failed to establish standing.

B. Plaintiffs' Speculation Also Does Not Establish Irreparable Harm

For the same reasons that Plaintiffs have failed to demonstrate sufficient injury to support standing, they have failed to meet their burden to show that they will be irreparably harmed absent preliminary injunctive relief. *See Faiveley Transp.*, 559 F.3d at 118. As discussed above, Plaintiffs' claim that the telephony metadata program is being used to build a "rich profile of every citizen" lacks evidentiary support.[6] Moreover, Plaintiffs have not established that the call detail records provided to NSA by telecommunications service providers will be queried for information about calls to or from persons with whom they communicate and that those persons will, in turn, be dissuaded from contacting Plaintiffs by phone. Put simply, Plaintiffs have no

[6] Plaintiffs rely on two cases involving disclosure of private data in support of their assertions of irreparable harm, Pls.' PI Br. at 37-38, but neither supports such a finding here. Both cases, *Hirschfeld v. Stone*, 193 F.R.D. 175, 185-86 (S.D.N.Y. 2000), and *Slevin v. City of New York*, 477 F. Supp. 1051 (S.D.N.Y. 1979), involved the disclosure of the content of private information, which is not at issue here. In *Hirschfeld*, the Court preliminarily enjoined a state agency from disclosing the content of sensitive psychiatric records of criminal defendants undergoing examinations to determine their fitness for trial. 193 F.R.D. at 192-93. Similarly, in *Slevin*, the statute at issue required certain city officials to publicly disclose personal financial data. 477 F. Supp. 2d at 1053-54. Unlike those cases, the instant matter does not involve the disclosure, or even the collection, of the content of any telephone conversation. Moreover, only a very small subset of the metadata the NSA obtains under the telephony metadata program is reviewed by NSA analysts, and then only in strictly controlled circumstances for a very limited counter-terrorism purpose. Thus, neither case supports Plaintiffs' claim of irreparable harm.

competent evidentiary support for their claim that they will suffer the harms they assert absent a preliminary injunction.[7]

POINT II: PLAINTIFFS CANNOT DEMONSTRATE THEY ARE LIKELY TO SUCCEED IN THIS ACTION BECAUSE THE NSA'S BULK COLLECTION OF TELEPHONY METADATA IS AUTHORIZED UNDER SECTION 215

Plaintiffs' request for a preliminary injunction must also be denied because they have no likelihood of prevailing on the merits of their claims. Indeed, Defendants have shown in their motion to dismiss that Plaintiffs' claims must be dismissed as a matter of law. Plaintiffs advance no arguments in support of their statutory or constitutional claims that demonstrates otherwise.

A. Judicial Review of Plaintiffs' Claim That the NSA's Bulk Collection of Telephony Metadata Exceeds Its Statutory Authority Is Implicitly Precluded

Plaintiffs first maintain that the NSA's bulk collection of telephony metadata exceeds the Government's statutory authority, within the meaning of the Administrative Procedure Act (APA), 5 U.S.C. § 706(2). This claim fails at the threshold because, as Defendants have already shown, judicial review of this claim is implicitly precluded by 18 U.S.C. § 2712 (authorizing suits for money damages against the United States for violations of three specific provisions of FISA, *not* including Section 215), and by Section 215 itself (providing for review of production orders only at the behest of recipients). As such, Plaintiffs' statutory claim lies beyond the scope

[7] Plaintiffs incorrectly argue that irreparable injury may be "presumed" in cases alleging constitutional deprivations. Pls.' PI Br. at 36 (citing cases). But the cases cited that rely on a "presumption" of irreparable harm pre-date the Second Circuit's decision in *Salinger*, where the court held that, in light of *eBay, Inc. v. MercExchange, LLC*, 547 U.S. 388 (2006) and *Winter*, "courts must not simply presume irreparable harm." *Salinger*, 607 F.3d at 82. Although a First or Fourth Amendment violation may, if proven, amount to irreparable injury, Plaintiffs still must demonstrate that such a violation has occurred, or imminently will occur, *id*., a task which they have failed to accomplish for the reasons stated above. *Cf. Ligon v. City of New York*, 925 F. Supp. 2d 478, 539 (S.D.N.Y. 2013) (constitutional violation found to be irreparable harm in light of evidentiary showing).

of the APA's waiver of sovereign immunity, and is jurisdictionally barred. Defs.' MTD at 14-19.

B. Plaintiffs' Claim That the NSA's Bulk Collection of Telephony Metadata Exceeds Its Statutory Authority Under Section 215 Is Also Unlikely to Succeed on the Merits

Even if judicial review of Plaintiffs' statutory claim were not precluded, the claim lacks merit. Section 215 authorizes the FISC to issue an order for the "production of any tangible things" upon application by the FBI "showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized [counter-terrorism] investigation" 50 U.S.C. § 1861(a)(1)(A), (b)(2)(A). Plaintiffs maintain that the NSA's bulk collection of telephony metadata disregards this requirement. But since May 2006, fourteen separate judges of the FISC have concluded on thirty-four occasions that the FBI satisfied this requirement, finding "reasonable grounds to believe" that the telephony metadata sought by the Government "are relevant to authorized investigations … being conducted by the FBI … to protect against international terrorism." Holley Decl. ¶¶ 6, 11; *see* Primary Order at 1; Aug. 29 FISC Op. at 11. Only recently the FISC concluded that

> [b]ecause known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, the production of the information sought meets the standard for relevance under Section 215.

Aug. 29 FISC Op. at 18.

Considering that the Government has consistently demonstrated the relevance of the requested records to the FISC's satisfaction, as Section 215 requires, it is difficult to understand how the Government can be said to have acted in excess of statutory authority. At bottom, Plaintiffs are asking this Court to conclude that the FISC exceeded *its* authority when it authorized the NSA's bulk collection of telephony metadata, and that this Court (without the

benefit of the classified applications and information available to the FISC, *see* Holley Decl. ¶¶ 10-11) should substitute its judgment for the decisions that the FISC reached thirty-four times.

In support of their position, Plaintiffs observe that in criminal proceedings "district courts review the lawfulness of FISC orders" authorizing electronic surveillance, and that "courts often examine the legality of search or arrest warrants" issued by coordinate courts. Pls.' PI Br. at 8 n.8. But Plaintiffs invoke these precedents without acknowledging the standard of review applied in such situations. For example, judicial review of FISA warrants is "deferential," involving only "minimal scrutiny by the courts." *United States v. Abu-Jihaad*, 630 F.3d 102, 130 (2d Cir. 2010). More to the point here, when courts are called on to enforce grand jury or administrative subpoenas – instruments that informed Congress's understanding of Section 215, *see* Defs.' MTD at 23 – the Government's determination that records are "relevant" to its investigation is subject only to the most deferential review.[8]

An equally deferential standard of review is called for in this context, where ensuring the Government's access to the information needed to carry out its national security mission is imperative, and where deferential review is commanded by the terms of Section 215 itself. Section 215 conditions the Government's access to business records, not on a showing of relevance, but on a showing of "*reasonable grounds to believe* that the [records] are relevant" to authorized counter-terrorism investigations. 50 U.S.C. § 1861(b)(2)(A) (emphasis added), (c)(1). Under this standard, in order to find that the FISC's production orders exceeded its authority, this

[8] *See United States v. R. Enters., Inc.*, 498 U.S. 292, 301 (1991) (grand jury subpoena challenged on relevancy grounds must be upheld unless "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation"); *NLRB v. Am. Med. Response, Inc.*, 438 F.3d 188, 193 (2d Cir. 2006) (in a proceeding to enforce an administrative subpoena, "the agency's appraisal of relevancy" to its investigation "must be accepted so long as it is not obviously wrong," and the "district court's finding of relevancy" will be affirmed unless it is "clearly erroneous").

Court would have to conclude that the fourteen FISC judges who repeatedly issued those orders lacked any reasonable basis for doing so. That proposition is self-defeating. The fact that fourteen judges of the FISC have granted the FBI's applications for bulk production of telephony metadata should itself demonstrate that the grounds advanced by the Government for believing these records to be relevant to authorized counter-terrorism investigations are, at the very least, reasonable. Plaintiffs offer no convincing arguments, in light of these repeated rulings, that they are likely to succeed in establishing otherwise.

Under the common legal usage that informs the meaning of relevance under Section 215, documents are considered relevant if they bear on, or reasonably could lead to information bearing on, the matter at hand. Defs.' MTD at 21-23. As Congress and the FISC have recognized, the concept of relevance under Section 215 must also extend "wide latitude" to the Government to seek and obtain the information needed to detect terrorist operatives and bring their plans to a halt before they strike. Aug. 29 FISC Op. at 18-19, 23; *see* Defs.' MTD at 25-26. Thus, bulk telephony metadata are pertinent (at the least) to FBI counter-terrorism investigations because, as experience has shown, they permit the use of analytical tools to detect contacts between foreign terrorists and their associates located in the United States who may be planning attacks. Holley Decl. ¶¶ 8-9, 18-26; Shea Decl. ¶¶ 44, 46-48. Targeted tools of investigation that do not involve bulk collection of the data cannot always achieve this objective as effectively, if at all, because the Government cannot know, in advance of linking a phone number (or other identifier) to a terrorist organization, where in the data the terrorists' communications can be found. Holley Decl. ¶¶ 9, 27-29; Shea Decl. ¶¶ 57-63. Absent bulk collection, it may not be feasible to identify chains of communications among terrorist operatives that extend across different time periods, or different providers' networks. Holley Decl. ¶ 9, 27-29; Shea Decl. ¶ 60.

In short, there are ample grounds for concluding that bulk telephony metadata are "relevant" to authorized investigations of international terrorism within the meaning of Section 215. That conclusion is reinforced, as the FISC recently recognized, by Congress's re-enactment of Section 215 without change in 2010 and 2011, after receiving notice that the FISC and the Executive Branch had interpreted Section 215 to authorize the bulk collection of telephony metadata. Aug. 29 FISC Op. at 23-28; *see also* Defs.' MTD at 26-28.

Plaintiffs argue that the "core problem" with this understanding of relevance is that most of the call detail records collected by the Government cannot be "tie[d]" to a specific counter-terrorism investigation. Pls.' PI Br. at 10. That observation hardly comes as a revelation. The Government has always acknowledged, and the FISC has understood, that the vast majority of the call detail records the Government expects to collect do not document communications between terrorist operatives. *See* Aug. 29 FISC Op. at 20-23. At the same time, the FISC has recognized that bulk collection of the data is necessary to the program – and therefore that the records are relevant as a whole – because the Government cannot know in advance of making authorized queries which communications occurring at what times, on which providers' networks, will reflect connections between terrorist groups and operatives located in the United States. *See id.* at 22. Thus, the collateral acquisition of records that do not pertain to such communications is not a "problem" with the Government's (and the FISC's) understanding of relevance, but an outgrowth of the necessarily wide latitude that Congress extended to the Government to obtain foreign intelligence information under Section 215. As the FISC has recognized, Congress anticipated that prospect and provided for the imposition of minimization procedures to safeguard against the improper use or dissemination of U.S.-person information produced under Section 215 orders. *Id.* at 11, 22-23; Defs.' MTD at 26 n.14; Shea Decl. ¶¶ 29-35.

Plaintiffs cite a patchwork of cases for the proposition that "courts routinely quash subpoenas for records that do not have a direct relationship to the underlying investigation they are meant to serve." Pls.' PI Br. at 11. The cited cases, however, do not substantiate the blanket rule that Plaintiffs posit.[9] To the contrary, under the accepted legal understanding of relevance in grand jury, civil, and administrative proceedings, courts have authorized the production of voluminous repositories of records, even where the odds of any particular record being directly relevant to the subject matter of the inquiry are small, so long as production of the records as a whole was reasonably likely to lead to the discovery of discrete amounts of information with a direct bearing on the subject matter of the investigation. Defs.' MTD at 22 & n.9; *see also In re Application of the United States*, 830 F. Supp. 2d 114, 130 (E.D. Va. 2011). While Plaintiffs maintain that there is "no support" in precedent in these traditional contexts for the production of data on the scale of bulk telephony metadata, Pls.' PI Br. at 8-9, in the counter-terrorism context at issue in this case, the FISC has upheld this collection under the law thirty-four times.

[9] For example, in *Bowman Dairy Co. v. United States*, 341 U.S. 214 (1951), the Court quashed (in part) a trial subpoena issued under Federal Rule of Criminal Procedure 17(c) because it attempted to convert Rule 17(c) into a tool for general discovery far outstripping its intended purposes. *Id.* at 220-21. *Cheney v. United States Dist. Court*, 542 U.S. 367, 387-88 (2004), involved burdensome and intrusive discovery requests served on the Vice President and other senior Government officials that threatened to interfere with the process by which the President obtained advice from those closest to him. *In re Horowitz*, 482 F.2d 72, 79-80 (2d Cir. 1973), enforced production of all documents within a specified data range without regard to subject matter unless it could be shown that particular documents had no conceivable relevance to the grand jury's inquiry. *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*, 846 F. Supp. 11 (S.D.N.Y. 1994), on which Plaintiffs lay particular emphasis, Pls.' PI Br. at 11-12, underscores the force of Defendants' position. There the Court quashed a grand jury subpoena for computer hard drives and floppy disks that contained both relevant and irrelevant information, because key-word searches of the information stored on the devices could identify relevant documents without requiring the production of irrelevant information. 846 F. Supp. at 12-13. Here, by contrast, it is not possible to isolate pertinent records in advance of production, because it cannot be known in advance which records reflect connections between known or suspected terrorists and others who may be working with them in the United States.

Also misdirected is Plaintiffs' remark that Section 215 should not be construed as a "license" for the Government to collect "virtually *any* record" on the theory that it may become relevant later. That is neither the premise nor the consequence of Defendants' position. The NSA collects bulk telephony metadata, not because they may become relevant, but because reason and experience teach that they are relevant, and fruitful, to the FBI's core mission of protecting national security. The NSA's analysis of bulk telephony metadata produces tips and leads that have given rise (or new impetus) to FBI counter-terrorism investigations. Holley Decl. ¶¶ 18, 20-26; Shea Decl. ¶¶ 44-56. To accept that fact is not to license the bulk collection of any records the Government chooses. The relevance of bulk telephony metadata is a function of distinctive characteristics not common to most other types of records, specifically their highly standardized and inter-connected nature, which makes them easily susceptible of analysis in large datasets to bring previously unknown connections between and among individuals to light. Shea Decl. ¶ 46; Felton Decl. ¶¶ 20-22. Both of these characteristics distinguish telephony metadata from such documents as medical records, or library-borrower records, which due to their non-standardized format and content are not readily susceptible of automated review and analysis and would not, in any event, enable the Government to identify otherwise unknown communications and relationships among individuals and organizations who may be planning terrorist attacks against this Nation.

In the final analysis, the "core problem" with Plaintiffs' position is that, apart from registering their own disagreement with the FISC's repeated determinations that bulk telephony metadata are relevant to FBI counter-terrorism investigations, they cite nothing in the text or legislative history of the statute demonstrating that the FISC, in reaching those conclusions, exceeded the authority that Congress intended it to wield. Congress assigned the FISC the responsibility of making relevance determinations under Section 215, and Plaintiffs have not

explained how the FISC has exercised that authority in a way, not simply that they object to, but that Congress did not intend.[10]

To the contrary, it is Plaintiffs' concept of relevance that cannot be squared with the intent of Congress. Plaintiffs suggest that Section 215 should be understood only to permit the collection of records that are themselves associated with terrorist organizations or activity. *See* Pls.' PI Br. at 10. Yet as Plaintiffs acknowledge, when Congress passed the USA PATRIOT Act in 2001, it expanded the Government's authority to obtain business records under FISA by eliminating the requirement in prior law 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." 50 U.S.C. § 1862(b)(2)(B) (2000 ed.); Pub. L. 107-56, § 215, 115 Stat. 288; Pls.' PI Br. at 3-4; *see* Aug. 29 FISC Op. at 13. In 2006, when Congress codified Section 215's relevance requirement, it rejected a proposal to restrict the statute's scope to records pertaining to individuals suspected of terrorist activity. *See* Defs.' MTD at 24 n.13. To read such a requirement into Section 215 now would be to flout, not execute, the will of Congress.[11]

---

[10] Plaintiffs argue that that the NSA's bulk collection of telephony metadata, followed by queries of the data under the "reasonable, articulable suspicion" standard, effectively shifts the task of making relevance determinations from the FISC to the Government, contrary to Congress's intent. Pls.' PI Br. at 15-16. This complaint adds nothing to Plaintiffs' case, as it reflects nothing more than their dissatisfaction with the determinations the FISC has consistently made, over the past seven years, that the telephony metadata as a whole are relevant to the Government's counter-terrorism investigations. As the FISC itself has observed, bulk collection of telephony metadata "fits comfortably within [the] statutory framework" of Section 215, which is "designed to permit the government wide latitude to seek the information it needs to meet its national security responsibilities … in combination with specific procedures for the protection of U.S. person information." Aug. 29 FISC Op. at 23.

[11] Plaintiffs cite recent statements by several Members of Congress indicating their disagreement with the Government's (and the FISC's) interpretation of Section 215 as authorizing the bulk collection of telephony metadata. Pls.' PI Br. at 9 n.9; *see also* Brief *Amicus Curiae* of Congressman F. James Sensenbrenner, Jr., in Support of Plaintiffs (Dkt. No. 56) at 1-2. Isolated statements by individual Members of Congress, even the sponsors of a measure, made after the enactment of a statute under consideration are entitled to little weight in

Plaintiffs raise two additional grounds on which they maintain that bulk collection of telephony metadata exceeds the Government's authority under Section 215, but both are plainly insubstantial and cannot support an award of preliminary relief. Plaintiffs first contend that the FISC may not prospectively direct the production of business records that do not yet exist, Pls.' PI Br. at 14, but Defendants have already explained that nothing in the text or legislative history of Section 215 suggests that the FISC may not require the production of records created during the lifespans of its orders. *See* Defs.' MTD at 30.[12] This approach does not provide the Government with indefinite access to bulk telephony metadata, as Plaintiffs suggest; the Government must obtain a new order for production of these metadata every 90 days.[13]

Plaintiffs also invoke the canon of construction that a "specific statute … controls over a general provision" in the event of a conflict between the two, *In re Stoltz*, 315 F.3d 80, 93 (2d Cir. 2002), and argue that the Government is relying on Section 215 to engage in conduct that is "disallow[ed]" by 50 U.S.C. § 1842, FISA's pen-register and trap-and-trace (PR/TT) provision.

---

discerning the intent of the Congress that adopted the measure as law. *Consumer Prod. Safety Comm. v. GTE Sylvania, Inc.*, 447 U.S. 102, 117-18 (1980); *Southeastern Cmty. Coll. v. Davis*, 442 U.S. 397, 411 n.11 (1979).

[12] This Court and others have held, analogously, that the Government may obtain prospective disclosure of non-content cell-phone service records under the Stored Communications Act, because nothing in the text or legislative history of that statute contains an "explicit limit on the disclosure of prospective data." *In re Application of the United States*, 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006). *See also United States v. Booker*, 2013 WL 2903562, *6-7 (N.D. Ga. June 13, 2013); *In re Application of the United States*, 632 F. Supp. 2d 202, 207 & n.8 (E.D.N.Y. 2008); *In re Application of the United States*, 622 F. Supp. 2d 411, 418-19 (S.D. Tex. 2007); *In re Application of the United States*, 433 F. Supp. 2d 804, 806 (S.D. Tex. 2006); *In re Application of the United States*, 411 F. Supp. 2d 678, 680 (W.D. La. 2006); *In re Application of the United States*, 405 F. Supp. 2d 435, 446-47 (S.D.N.Y. 2005).

[13] Furthermore, Section 215 expires on June 1, 2015, pursuant to section 102(b)(1) of the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, 120 Stat. 195 (50 U.S.C. § 1805 note), as amended by section 2(a) of the PATRIOT Sunsets Extension Act of 2011, Pub. L. 112-4, 125 Stat. 216. Congress will have to decide before then whether to re-enact Section 215 without change, or amend it, in light of what is now publicly known about the Government's exercise of authority under the statute.

Pls.' PI Br. at 14. Plaintiffs fail to explain how the Government's conduct in these circumstances would be "disallow[ed]" by section 1842, or to explain, for that matter, how section 1842 could be construed in the first place as a "more specific" statute dealing with the same subject matter as Section 215. Both are equally specific provisions that set forth the respective terms and conditions the Government must comply with to make use of two separate and distinct means of gathering foreign intelligence – the collection of business records, and the installation of PR/TT devices on the facilities of electronic and telephonic communications service providers. It is true that PR/TT devices can also be used to collect telephony metadata, but Plaintiffs cite nothing in the text or legislative history of section 1842 indicating that Congress intended PR/TT devices to be the exclusive means of collecting such information. *See* cases cited in footnote 15, *infra*.

In sum, Plaintiffs have not shown a substantial likelihood of prevailing on their claim that bulk collection of telephony metadata exceeds the Government's authority under Section 215.

POINT III: PLAINTIFFS CANNOT DEMONSTRATE THAT THEY ARE LIKELY TO SUCCEED ON THEIR FOURTH AMENDMENT CLAIM

Critical to Plaintiffs' argument that the collection of telephony metadata under Section 215 violates their Fourth Amendment rights is the premise that the NSA also collects and analyzes subscriber-identifying information – that is, to whom the phone numbers making and receiving a call belong – in addition to purely numerical information (the phone numbers dialed, the time and duration of calls made). As explained above, however, under the FISC orders at issue, the NSA collects no information identifying the persons to whom phone numbers belong. Moreover, under the FISC's orders, no metadata can be examined except the tiny fraction of the records that are responsive to authorized queries made under the "reasonable, articulable suspicion" standard. Such queries, even when made, are conducted solely to detect communications with unknown terrorist operatives and to provide the FBI and other agencies

with discrete information useful to their counter-terrorism mission, not to create profiles of ordinary Americans' lives.

Once its premise falls away, Plaintiffs' Fourth Amendment argument fails. There is no reasonable expectation of privacy in telephony metadata – all that is at issue here – as the Supreme Court squarely held in *Smith v. Maryland*, 442 U.S. 735 (1979). Thus, the telephony metadata program involves no Fourth Amendment search. Even if there were a search, it would be reasonable. Any intrusion on privacy is minimal, again because only telephony metadata are collected, and is outweighed in any event by the paramount Government interest in thwarting terrorist attacks.

A. Collection and Query of Telephony Metadata Does Not Constitute a Search

As set forth in Defendants' motion to dismiss, Plaintiffs' Fourth Amendment claim is controlled by *Smith*, which held that the Government's recording of the numbers dialed from an individual's home telephone, through the off-site installation of a pen register, did not constitute a search under the Fourth Amendment. *See also* Aug. 29 FISC Op. at 6 ("The production of telephone service provider metadata is squarely controlled by *Smith* . . . . [*Smith*] and its progeny have governed Fourth Amendment jurisprudence with regard to telephony and communications metadata for more than 30 years."). *Smith* held that individuals have no reasonable expectation of privacy in the telephone numbers they dial, because they convey the numbers to the phone company in the act of dialing, and "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." 442 U.S. at 743-44. *Smith* directly applies here to the collection of telephone numbers and other telephony metadata that subscribers voluntarily turn over to providers. Plaintiffs' attempts to distinguish *Smith* are unavailing.

Plaintiffs seek to avoid *Smith*'s holding by first alleging a subjective expectation of privacy in their telephony metadata, claiming to regard the mere *fact* of many of their calls as

sensitive or confidential. Pls.' PI Br. at 17-18. But under the FISC's orders the NSA may collect only phone numbers, and other numeric data, that do not identify who places or receives calls. Shea Decl. ¶¶ 15, 21; Holley Decl. ¶¶ 7, 11. Without that information, a phone number by itself does not reveal whether the number dialed is an abortion clinic, a criminal-defense lawyer, or a suicide hotline, or that the person placing the call is a whistleblower. The call detail records instead merely show that one ten-digit number called another. *See* Felton Decl. ¶ 20.[14]

Plaintiffs further claim, again contrary to *Smith*, that an expectation of privacy in dialed telephone numbers is objectively reasonable. The *Smith* Court held that "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as "reasonable."'" 442 U.S. at 743 (quoting *Katz v. United States*, 389 U.S. 347, 361 (1967)). The rationale for the holding was that the Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," such as, in *Smith*, the numbers a subscriber conveys to the phone company. *Id.* at 743-44. In the more than thirty years since *Smith* was decided, the strength of the third-party doctrine has not waned. *See* Defs.' MTD at 33. And the third-party doctrine has consistently been applied, both pre- and post-*Smith*, to telephone call detail records like the business records at issue here, which are also third-party

[14] The dissenters in *Smith* made the very argument now taken up by Plaintiffs – that the numbers dialed from a phone are "not without 'content'" and 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." *Smith*, 442 U.S. at 748 (Stewart, J., dissenting). The Court nonetheless ruled that there is no reasonable expectation of privacy in telephone numbers dialed. *Id*. at 741-42. Thus, while Plaintiffs attempt to make much of technological advances since *Smith* was decided that enable the analysis of large quantities of data, it is irrelevant under *Smith* that telephone numbers "could" be used to reveal intimate information.

Plaintiffs' further argument that they take measures to protect the "substance" (*i.e.*, content) of their communications from surveillance by the Government or other third parties, Pls.' PI Br. at 18, was also made and rejected in *Smith*. 442 U.S. at 743.

records.[15] Nor is there any reason to think that a subjective expectation of privacy in telephony metadata is any more reasonable now than it was in 1979. Just as they did in 1979, subscribers now "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.[16]

Plaintiffs seek to distinguish *Smith*'s holding by arguing that their "expectation that their telephony metadata will not be subject to long-term recording and aggregation by the government is objectively reasonable." Pls.' PI Br. at 18. But that assertion, like their claimed subjective expectation of privacy, relies on the erroneous and unsupported assumption that, under the FISC's orders, the metadata produced by telecommunications service providers to the NSA contain or reveal subscriber-identifying information. In support of their argument, Plaintiffs claim that "[t]he kind of surveillance at issue here permits the government to assemble a richly detailed profile of every person living in the United States and to draw a comprehensive map of their associations with one another." *Id.* That is not true. As explained above, when it

---

[15] *See, e.g., 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). *Cf. United States v. Covello*, 410 F.2d 536, 540-42 (2d Cir. 1969); *United States v. Gallo*, 123 F.2d 229, 231 (2d Cir. 1941).

[16] Plaintiffs' citation to their Verizon contracts, in which Verizon agrees to protect the confidentiality of certain customer information, including local and toll billing information, is not helpful to them. Pls.' PI Br. at 18 n.15. Plaintiffs concede that their agreement is qualified by the words "in accordance with applicable laws, rules and regulations," *id.*, and this case involves a court order to produce records. *See also* Verizon Privacy Policy at 3, available at http://www22.verizon.com/about/privacy/policy/ ("We may disclose information that individually identifies our customers or identifies customer devices in certain circumstances, such as: to comply with valid legal process including subpoenas, court orders or search warrants"). Nor is a provider's agreement to keep the information confidential legally relevant. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984); *United States v. Miller*, 425 U.S. 435, 443 (1976) ("the Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

collects telephony metadata under Section 215, the NSA receives no identifying information about subscribers, or the persons with whom they speak. Furthermore, under the FISC's orders, NSA analysts cannot access the data they receive except pursuant to queries based on telephone identifiers that are reasonably suspected of being associated with foreign terrorist organizations. Even when the database is queried with an authorized identifier, the NSA applies signals intelligence analysis to identify and alert the FBI to those communications that may be indicative of contacts between known or suspected terrorists and others who may be working with them in this country. This simply does not constitute an attempt to assemble a "richly detailed profile" on anyone. Moreover, when NSA alerts the FBI to particular communications, any subscriber-identifying information must be obtained from other sources, if necessary pursuant to other legal authorities.

For this reason as well, Plaintiffs' reliance on the two concurrences in *United States v. Jones*, 132 S. Ct. 945 (2012), which opined on expectations of privacy concerning long-term GPS monitoring, Pls.' PI Br. at 20, is misplaced. As an initial matter, this Court is obviously bound only by the majority opinion in *Jones*, not by the concurring opinions (one by Justice Alito and one by Justice Sotomayor).[17] In any event, the concerns expressed in the *Jones* concurrences do not apply to the NSA's telephony metadata program. As quoted by Plaintiffs, Justice Sotomayor expressed concern that the GPS monitoring at issue in *Jones* "'generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail

[17] *See United States v. Graham*, 846 F. Supp. 2d 384, 394 (D. Md. 2012) (noting that court must "proceed with caution in extrapolating too far from the Supreme Court's varied opinions in *Jones*. Until the Supreme Court . . . definitively conclude[s] that an aggregation of surveillance records infringes a Fourth Amendment legitimate expectation of privacy, this Court must apply the facts of this case to the law as currently interpreted."); *Ohio v. LeMasters*, 2013 WL 3463219, at *3 (Ohio App. 12 Dist. July 8, 2013) (court is "bound only by the majority opinion of the court [in *Jones*], rather than [by] questions raised and suggestions made within the dicta of concurring opinions.").

about her familial, political, professional, religious, and sexual associations.'" Pls.' PI Br. at 20 (quoting *Jones*, 132 S. Ct. at 955-56) (Sotomayor, J., concurring)). That was so because the GPS device used in *Jones* was attached by law enforcement officers to a single, known person's vehicle and recorded the vehicle's locations over a period of time. Law enforcement learned from the GPS data where that particular person had been over 28 days and used that information to prosecute him. In contrast here, as discussed above, the telephony metadata program provides the NSA with information about calls between unidentified phone numbers, when the calls occurred, and how long the calls lasted. Thus, unlike in *Jones*, the NSA does not know the identity of anyone making or receiving the calls, and under the terms of the FISC's orders, cannot use the metadata to draw comprehensive maps of individuals' associations.[18]

Even if it were otherwise, Plaintiffs have offered no evidence that the NSA or the FBI has ever viewed any metadata of *their* communications, let alone analyzed those data to map their associations. Plaintiffs not only have no support for their claim that the NSA programmatically collects subscriber-identifying information and analyzes it to create "richly detailed profile[s]" of persons living in the United States, they also have not shown that the NSA has done so with metadata of *their* calls. Even if the practices they hypothesize were taking place and violated

[18] Plaintiffs' suggestion that the *Jones* concurrences somehow overruled the third-party doctrine that supplied the controlling rationale in *Smith*, Pls.' PI Br. at 23 n.18, is also meritless. *See Graham*, 846 F. Supp. 2d at 403 ("unless and until the Supreme Court affirmatively revisits the third-party doctrine, the law is that 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,'" quoting *Smith*, 442 U.S. at 743-44). The additional cases Plaintiffs cite as undermining the third-party doctrine do nothing of the sort; they do not even involve situations in which the items or information obtained by the government had been voluntarily turned over to a third party. *Florida v. Jardines*, 133 S. Ct. 1409, 1413 (2013) (drug-sniffing dog on defendant's porch detected odors indicating the presence of marijuana inside the home); *Kyllo v. United States*, 533 U.S. 27, 29-30 (2001) (police aimed thermal-imaging device at defendant's home to detect heat emanating from inside); *Ferguson v. City of Charleston*, 532 U.S. 67, 84-85 (2001) (state hospital drug-screened patients' urine samples for law-enforcement purposes); *Bond v. United States*, 529 U.S. 334, 335 (2000) (police squeezed bus passenger's bag placed in overhead storage space).

individuals' legitimate expectations of privacy, the lack of any evidence that *Plaintiffs* have been the subject of such practices is fatal to their Fourth Amendment claim. *Rakas v. Illinois*, 439 U.S. 128, 133-38 (1978) (Fourth Amendment rights are personal rights which may be enforced only at the instance of one whose own protection has been infringed by the alleged search); *United States v. Haqq*, 278 F.3d 44, 47 (2d Cir. 2002) (an individual's Fourth Amendment rights are violated only when the challenged conduct invaded his legitimate expectation of privacy rather than that of a third party).

Plaintiffs' emphasis on the breadth of the telephony metadata program – *i.e.*, the fact that under the program, telecommunications service providers provide the NSA with the call detail records of millions of Americans – does not alter that conclusion. The personal nature of Fourth Amendment rights precludes the argument that Plaintiffs' rights are violated by virtue of any collection or analysis of metadata pertaining to the calls of other persons. *See* Defs.' MTD at 35. *See also* Aug. 29 FISC Op. at 8 ("[W]here one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."). Nor is the fact that the collection is authorized for a period of 90 days material to this question. In *Miller*, 425 U.S. at 437-38, for example, the Court upheld a subpoena for all records of all bank accounts belonging to Miller, for a period of almost four months. *See also Doe*, 537 F. Supp. at 839 (ordering phone company to produce telephone records of a subscriber for six months).

Given the conclusive, controlling effect of *Smith* on this case, there is no likelihood that Plaintiffs will succeed on the threshold question presented by their Fourth Amendment claim – whether a search occurred. *See* Aug. 29 FISC Op. at 9 ("there is no legal basis" for finding that the bulk telephony metadata collection violates the Fourth Amendment).

B. The NSA's Bulk Collection of Telephony Metadata is Reasonable

As also established in Defendants' motion to dismiss, even if the collection and retention of Plaintiffs' telephony metadata constituted a search under the Fourth Amendment, it is reasonable when the minimal intrusion on privacy that may result from the collection of purely numerical information is weighed against the substantial governmental interest in preventing terrorist attacks. Defs.' MTD at 35-37. *See also* Shea Decl. ¶¶ 6-8, 10; Holley Decl. ¶¶ 4-5, 20-26.[19]

Plaintiffs' primary attack on the reasonableness of the program is to assert it is a "general warrant for the digital age." Pls.' PI Br. at 23. But the cases Plaintiffs rely on for this comparison are inapposite. *Id*. at 23-28 (relying on *Berger v. State of New York*, 388 U.S. 41 (1967); *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297 (1972); *United States v. Tortorello*, 480 F.2d 764 (2d Cir. 1973); *United States v. Bobo*, 477 F.2d 974 (4th Cir. 1973); *United States v. Cafero*, 473 F.2d 489 (3d Cir. 1973)). Those cases involved the authorization of electronic eavesdropping on the contents of private conversations, a far greater intrusion on privacy interests than the collection of numerical telephony metadata devoid of any subscriber-identifying information or substantive content. *See, e.g.*, *Smith*, 442 U.S. at 741; *Keith*, 407 U.S. at 320 ("Official surveillance . . . risks infringement of constitutionally protected privacy of speech."); *Berger*, 388 U.S. at 63 ("[I]t is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded."). Nor does the program at issue here even involve electronic surveillance, as that term is defined by FISA (*see* 50 U.S.C. § 1801); the orders require the

[19] Plaintiffs state in their brief that they are not addressing the "special needs" doctrine. Pls.' PI Br. at 24. But the balancing of the intrusion on privacy interests against the promotion of legitimate governmental interests employed by plaintiffs to assess reasonableness of the telephony metadata program tracks the balancing test used in the special needs context. *Compare id*., *with* Defs.' MTD at 35.

production of providers' business records. Thus, Plaintiffs' invocation of a heightened standard of reasonableness in the context of electronic surveillance is inapplicable here.

Also contrary to Plaintiffs' arguments, the orders issued by the FISC approving the telephony metadata collection cannot be condemned as "roving commissions," Pls.' PI Br. at 23-24, inasmuch as they (1) specifically describe the records to be provided (call detail records, or telephony metadata, as defined by the orders), (2) are addressed to particular telecommunications service providers, (3) are issued for a finite period of time (90 days), and (4) heavily restrict the use, retention, and dissemination of the records collected. *See* Primary and Secondary Orders, Shea Decl. Exhs. A & B; Shea Decl. ¶¶ 14-15; Holley Decl. ¶¶ 6-7, 12-13; *Berger*, 388 U.S. at 56-60. *See also Maryland v. King*, 133 S. Ct. 1958, 1980 (2013) (taking into account restrictions on a program in assessing its reasonableness). Lastly, while Plaintiffs contend that the telephony metadata program is unbounded in that "[t]he government simply obtains all of Plaintiffs' phone records, no matter their relevance to an ongoing investigation," Pls.' PI Br. at 27, as explained above, bulk telephony metadata are relevant to authorized investigations against international terrorism, as the FISC has repeatedly found.

In addition, the telephony metadata program is at the least a "reasonably effective means" of promoting the Government's counter-terrorism goals. *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls*, 536 U.S. 822, 837 (2002). The program enhances the Government's ability to identify and track terrorist operatives who might otherwise elude detection, and has contributed to counter-terrorism investigations. Without the bulk collection of telephony metadata, the Government's ability to detect communications between known or suspected terrorists and others who may be engaged in terrorist activity could be impaired. Thus, the program is more effective than if the Government "simply collect[ed] those records relating

to [particular suspected terrorists]." Pls.' PI Br. at 28. *See* Shea Decl. ¶¶ 57-63; Holley Decl. ¶¶ 9, 27-29.

For the foregoing reasons, Plaintiffs' Fourth Amendment claim has no likelihood of success on the merits.

POINT IV: PLAINTIFFS CANNOT DEMONSTRATE THAT THEY ARE LIKELY TO SUCCEED ON THEIR FIRST AMENDMENT CLAIM

A. Plaintiffs' First Amendment Claim Fails Because Good-Faith Investigatory Conduct Not Intended to Deter or Punish Protected Speech or Association Does Not Violate the First Amendment

Plaintiffs likewise have failed to plausibly allege, and now to show, that the Government's collection of non-content telephony metadata violates the First Amendment. As Defendants have already explained, good-faith governmental investigations conducted in observance of the Fourth Amendment, without the purpose of deterring or penalizing protected speech or association, do not violate the First Amendment. *See* Defs.' MTD at 37-38. Because Plaintiffs do not contend, much less offer any proof, that the telephony metadata program is directed at them based on their expressive or associational activities, their First Amendment claim fails as a matter of law, and cannot serve as a predicate for issuing a preliminary injunction. *Id.* at 38-40.

B. Because the Telephony Metadata Program Imposes No Direct or Significant Burden on Plaintiffs' Associational Rights, the "Exacting Scrutiny" Test Does Not Apply

Plaintiffs' contention that the telephony metadata program should be subjected to "exacting scrutiny" because it imposes a "significant burden" on Plaintiffs' associational rights, Pls.' PI Br. at 29-36, also fails as a matter of law and fact. First, as discussed above, the underlying premise of Plaintiffs' argument – that the program exposes all of Plaintiffs' sensitive contacts with members, donors, clients, whistleblowers, and others with whom they collaborate in their work to government scrutiny – is without foundation. Plaintiffs do not allege, and do not

offer any evidence, that the metadata of any of their communications – which do not include the names or addresses of anyone with whom Plaintiffs speak by phone – have ever been accessed or reviewed by NSA analysts for any purpose, whether as the results of queries based on the "reasonable, articulable suspicion" standard, or otherwise.

Furthermore, Plaintiffs have set forth no evidence of an actual "chilling effect" attributable to the telephony metadata program that interferes with their rights of association. Plaintiffs do not contend that they themselves are actually or even subjectively chilled by the telephony metadata program. Rather, they express their belief that others who regard their associations with Plaintiffs as confidential may be "chilled" from contacting them. *See* Compl. ¶¶ 3, 35; Pls.' PI Br. at 33-34; German Decl. ¶¶ 29-30; Dunn Decl. ¶ 9; Shapiro Decl. ¶ 8. Plaintiffs provide no concrete example, however, to substantiate their assertion that prospective clients, or others with whom they work, have become unwilling or even reluctant to contact them because of the telephony metadata program. Instead, they offer only general predictions of such a possibility. *See* German Decl. ¶ 29 (speculating that knowledge of the Program "will cause some individuals to remain silent rather than contact me or the ACLU"), *and id.* ¶ 30 ("some individuals may decide not to seek advice from me or the ACLU"); Shapiro Decl. ¶ 8 (speculating similarly as to this "genuine risk").

These allegations fail to demonstrate an actual chill on associational activity as required to support a First Amendment claim. *See Curley v. Vill. of Suffern*, 268 F.3d 65, 73 (2d Cir. 2001) ("Where a party can show no change in his behavior, he has quite plainly shown no chilling of his First Amendment right to free speech."); *Fighting Finest, Inc. v. Bratton*, 95 F.3d 224, 228 (2d Cir. 1996) (rejecting freedom of association claim where plaintiff "ha[d] not alleged that the actions of [the government] caused its members to suspend or even curtail their associational activities"). As Defendants have explained, *see* Defs.' MTD at 39, even if

government conduct makes it incidentally "more difficult for individuals to exercise their freedom of association," that "does not, without more, result in a violation of the First Amendment." *Fighting Finest*, 95 F.3d at 228. Rather, "[t]o be cognizable, the interference with associational rights must be 'direct and substantial' or 'significant." *Id.* (quoting *Lyng v. UAW*, 485 U.S. 360, 366, 367 & n.5 (1988)). Plaintiffs have not made that showing here.

Nor can Plaintiffs draw any meaningful parallel between this case and compelled disclosure cases where courts have applied "exacting" First Amendment scrutiny to government conduct. In *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958), on which Plaintiffs principally rely, Pls.' PI Br. at 31-32, the Alabama courts had ordered the NAACP to produce local membership lists in connection with litigation to oust it from the State as an unregistered corporation. *See* 357 U.S. at 451-53. The Supreme Court held that Alabama could not compel the NAACP to disclose its membership lists because it "made an uncontroverted showing that on past occasions revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility." *Id.* at 462. "Under these circumstances," the Court found it "apparent that compelled disclosure of [NAACP]'s Alabama membership" entailed a "substantial restraint" on the organization's freedom of association. *Id.*; *see also Brown v. Socialist Workers '74 Campaign Comm.*, 459 U.S. 87, 98-99 (1982) (similarly holding unconstitutional the targeted, compelled disclosure of contributions to and expenditures by Socialist Workers Party, based on "substantial evidence" of harassment, threats, assaults, and reprisals against its members); *Bates v. City of Little Rock*, 361 U.S. 516, 523-24 (1960) (similar).

In contrast, the FISC's orders authorizing the telephony metadata program do not compel Plaintiffs to disclose, or direct anyone else, including telecommunications service providers, to disclose names or addresses of Plaintiffs, their members, their clients, or anyone else with whom

they associate (or expose them to the public hostility suffered by the parties in such cases as *NAACP*). The NSA obtains only numeric telephony metadata, to which analysts and investigators are permitted no access unless they are responsive to queries based on identifiers associated with foreign terrorist organizations. Plaintiffs have neither alleged nor shown that any metadata of their calls have been retrieved or examined by NSA analysts as a result of such queries, or otherwise.

Moreover, even if this were a compelled-disclosure case, Plaintiffs could not establish the "substantial evidence" of a direct and targeted encroachment on First Amendment rights required to trigger "exacting scrutiny," as was the situation in many of the cases Plaintiffs cite.[20] As the Supreme Court has explained, "exacting scrutiny" applies "to regulations that suppress, disadvantage, or impose differential burdens upon speech *because of its content*." *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 642 (1994) (emphasis added); *see also Clark*, 750 F.2d at 94 (holding that exacting scrutiny is appropriate in police surveillance context, where "government

[20] For example, the court in *Clark v. Library of Congress* applied "exacting scrutiny" to a "targeted investigation of an individual based solely on the exercise of his associational rights," which resulted in "an extraordinary" full field investigation by the FBI. 750 F.2d 89, 95 (D.C. Cir. 1984). The court noted that Clark "based his claim on a significantly intrusive investigation for which he alone was singled out by the Library on the basis of his peaceful association with a lawful political association." *Id.* at 94. Similarly, the Second Circuit applied exacting scrutiny in *Tabbaa v. Chertoff* based on a finding that the plaintiffs established the requisite "direct and substantial" interference with their associational rights when they were forcibly "detained and searched for between four and six hours," their cars were searched, and they were "questioned, patted-down, fingerprinted, and photographed . . . solely by virtue" of having attended an Islamic conference. 509 F.3d 89, 92-95, 102 (2d Cir. 2007). *See also Elrod v. Burns*, 427 U.S. 347, 350 (1976) (applying "exacting scrutiny" test to First Amendment claim by public employees upon their termination "solely for the reason that they were not affiliated with or sponsored by the Democratic Party"); *In re Grand Jury Proceedings*, 776 F.2d 1099, 1102-03 (2d Cir. 1985) (rejecting, under "exacting scrutiny" test, free association challenge to targeted grand jury subpoena compelling individual's detailed testimony on the membership, structure, and funding of the Hell's Angels Motorcycle Club); *Local 1814, Int'l Longshoreman's Ass'n v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 269 (2d Cir. 1981) (applying "exacting scrutiny" test to government-compelled disclosure of longshoremen's political contributions).

action *is motivated solely by an individual's lawful beliefs or associations*") (emphasis added); *FEC v. Larouche Campaign*, 817 F.2d 233, 234 (2d Cir. 1987) (noting similarly where very purpose of investigation was the targeted association's political speech and activity).

Again, Plaintiffs do not allege or submit evidence that the telephony metadata program is content-based, much less directed at curtailing or punishing free expression or association. *See* Pls.' PI Br. at 30-36. Plaintiffs present no evidence indicating that the program is specifically directed at individuals or organizations because of their expressive or associational activities. To the contrary, as the record reflects, the program involves broad-based collection of telephony metadata for purposes – detecting terrorist communications, and preventing terrorist attacks – having nothing to do with activities protected by the First Amendment. Indeed, numerous safeguards built into the program prevent the Government from acquiring or using the data for purposes forbidden by the First Amendment.[21] Plaintiffs' failure to establish "direct and substantial" interference with their associational rights brings the First Amendment inquiry – under exacting scrutiny, or any other standard – to an end. *Tabbaa*, 509 F.3d at 101.[22]

---

[21] *See* Primary Order at 8-9 (requiring NSA OGC to review all findings of reasonable, articulable suspicion for phone numbers reasonably believed to be used by United States persons to ensure the findings are not based on activities protected by the First Amendment); 50 U.S.C. § 1861(a)(1) (prohibiting any investigation of a United States person "conducted solely upon the basis of activities protected by the first amendment to the Constitution"); *Attorney General's Guidelines for Domestic FBI Operations*, U.S. Dep't of Justice at 13 (Sept. 29, 2008) (same); Shea Decl. ¶¶ 21, 32.

[22] Plaintiffs' attempt to compare the Program to the "FBI's use of mail covers," which they term the "postal equivalent of 'metadata,'" Pls.' PI Br. at 31, is also unavailing. A mail cover is a process by which a record is made of any data appearing on the outside cover of mail to or from targeted individuals or organizations, including the name and address of the sender. *See* 39 C.F.R. § 233.3; *United States v. Bianco*, 534 F.2d 501, 507 (2d Cir. 1976). As the FISC's orders make clear, the program at issue here does not involve the targeted collection, recording, or analysis of any such identifying information. *See* Primary Order at 3 n.1; Shea Decl. ¶¶ 7, 15, 18; Holley Decl. ¶¶ 7, 11.

C. Even if "Exacting Scrutiny" Applied, the Telephony Metadata Program Serves the Government's Compelling Interest in Protecting National Security in a Manner That Is Not Practically Achievable by Other Means.

Even if Plaintiffs could make a case for applying exacting scrutiny, the telephony metadata program would pass muster. First, the program "serve[s] compelling state interests, unrelated to the suppression of ideas . . . ." *Tabbaa*, 509 F.3d at 102. It is undisputed that the telephony metadata program is directed at furthering the Government's compelling interest in identifying and tracking terrorist operatives and ultimately thwarting terrorist attacks. *See id.* at 103 ("[T]he government's interest in protecting the nation from terrorism constitutes a compelling state interest unrelated to the suppression of ideas . . . ."); Shea Decl. ¶¶ 6-8, 10; Holley Decl. ¶¶ 4-5.

Second, the Government has explained that the program's objectives could not be achieved through the alternative means that Plaintiffs suggest – collecting metadata associated only with the calls of persons already known to be, or suspected of being, terrorist operatives. *Tabbaa*, 509 F.3d at 102; Pls.' PI Br. at 34. Relying solely on such targeted collection of telephony metadata, whether by subpoenas, national security letters, or PR/TT devices, would hinder the Government's ability to identify networks of previously unknown foreign terrorist operatives in the United States as rapidly, reliably, and completely as analysis of bulk telephony metadata. *See* Holley Decl. ¶¶ 9, 27-29; Shea Decl. ¶¶ 57-63. Likewise, without its aggregation of bulk metadata, the NSA's ability to detect previously unknown chains of communications among terrorist operatives, crossing different time periods and provider networks, would be impaired. Information that has proven valuable in the past and could be important in the future to the initiation and advancement of FBI counter-terrorism investigations, and to the prevention of terrorist attacks, could also be lost. *See* Holley Decl. ¶¶ 9, 19-26; Shea Decl. ¶¶ 46, 57-63.

For all of these reasons, Plaintiffs' First Amendment claim, like their statutory and Fourth Amendment claims, fails to supply a predicate for awarding preliminary injunctive relief.

POINT V: THE BALANCE OF THE EQUITIES AND THE PUBLIC INTEREST REQUIRE THAT AN INJUNCTION BE DENIED

Finally, Plaintiffs have not demonstrated that the public interest or a balancing of the equities supports their requested injunction; to the contrary, such a balancing strongly militates against entering any injunction. For even if Plaintiffs could show irreparable harm, which they cannot, that harm would be outweighed by the public consequences of a preliminary injunction. The Supreme Court has required the courts to balance the irreparable harm to plaintiffs if injunctive relief is denied against the harm to the public interest if it is granted. *Winter*, 555 U.S. at 25. Indeed, the Court has instructed the lower courts to be particularly mindful of an injunction's "consequent adverse impact on the public interest in national defense." *Id.* This is yet further reason why Plaintiffs' request for preliminary relief should be denied.[23]

Plaintiffs seek a three-fold injunction (1) barring the Government from collecting Plaintiffs' call records under the Section 215 telephony metadata program; (2) requiring the Government to quarantine all of Plaintiffs' call records already collected under the program; and (3) prohibiting the Government from querying metadata obtained through the program using any phone number or other identifier associated with Plaintiffs. Pls.' PI Br. at 2. All three aspects of the injunctive relief Plaintiffs seek would, ironically, require the NSA to know which phone

[23] Injunctive relief is particularly inappropriate where, as here, the case involves professional judgments about national security matters. Great deference is given to the professional judgment of intelligence officials regarding such matters, and courts are properly reluctant to interfere with that judgment. *Holder v. Humanitarian Law Project*, 130 S. Ct. 2705, 2724 (2010) ("Everyone agrees that the Government's interest in combating terrorism is an urgent objective of the highest order."); *id*. at 2727 (according deference to Executive affidavits on issues of national security, and stating "evaluation of the facts by the Executive, like Congress's assessment, is entitled to deference [because t]his litigation implicates sensitive and weighty interests of national security"); *Winter*, 555 U.S. at 24 (similar).

numbers belong to or are associated with Plaintiffs. Shea Decl. ¶ 64. As noted throughout this brief, the NSA does not have that information under the telephony metadata program.

Even if Plaintiffs were to provide this information to the NSA, it would be burdensome to implement the requested injunction. Technical experts would have to develop the technical capability to remove those numbers from the database upon receipt of each batch of metadata, or to block the numbers from view when queries are run. To identify, design, build, and test such an implementation solution would potentially require the hiring of additional personnel and could take approximately six months. Once implemented, any potential solution could undermine the results of authorized queries by eliminating potential call chains. Moreover, if the injunction were to be lifted, the NSA would have to devise a way to reverse the implementation solution, which would require additional resources. *Id.* ¶ 65.

The impact of the requested injunction would of course be magnified if the issuance of the injunction were to precipitate additional successful requests for similar injunctions by large numbers of individuals and organizations. In that event, it is possible at some point that the cumulative interference with the NSA's ability to continue collecting and analyzing telephony metadata in the manner prescribed by the FISC's orders could have an adverse impact on the Government's ability to carry out its counter-terrorism mission. Shea Decl. ¶ 63.

CONCLUSION

For the reasons stated above and in Defendants' memorandum in support of their motion to dismiss, Plaintiffs' motion for a preliminary injunction should be denied.

Dated: New York, New York
October 1, 2013

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director

ANTHONY J. COPPOLINO
Deputy Director

By: /s/ James Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
BRYAN DEARINGER
Trial Attorney
Civil Division
Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Avenue, N.W.
Washington, DC 20001
Tel.: (202) 514-3358

PREET BHARARA
United States Attorney for the
Southern District of New York
Attorney for Defendants

By: /s/ David S. Jones
DAVID S. JONES
TARA M. La MORTE
JOHN D. CLOPPER
CHRISTOPHER HARWOOD
Assistant United States Attorneys
86 Chambers Street, 3rd Floor
New York, New York 10007
Tel. (212) 637-2739/2746/2716/2728
Fax (212) 637-2730
david.jones6@usdoj.gov
tara.lamorte2@usdoj.gov
john.clopper@usdoj.gov
christopher.harwood@usdoj.gov