IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LARRY KLAYMAN, *et al.*, Plaintiffs, v. BARACK OBAMA, President of the United States, *et al.*, Defendants.	Civil Action No. 1:13-cv-00851-RJL
LARRY KLAYMAN, *et al.*, Plaintiffs, v. BARACK OBAMA, President of the United States, *et al.*, Defendants.	Civil Action No. 1:13-cv-00881-RJL

GOVERNMENT DEFENDANTS' OPPOSITION TO
PLAINTIFFS' MOTIONS FOR PRELIMINARY INJUNCTIONS

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

REGULATIONS

INTRODUCTION

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 Government's exploitation of terrorist communications is a critical tool in this effort. Plaintiffs in these cases ask this Court to preliminarily enjoin important means by which the National Security Agency (NSA) has gathered information about communications among known and unknown terrorist actors in order to thwart future terrorist attacks. That request should be denied.

In Plaintiffs' telling, these activities constitute a single "mass surveillance program," called PRISM, in which the Government collects both "metadata" about and the contents of Americans' telecommunications, and exploits this information "to build comprehensive profiles of ordinary Americans" revealing intimate details about their lives and personal associations. Plaintiffs challenge these alleged intelligence-gathering activities—as they describe them—as exceeding the Government's authority under the Foreign Intelligence Surveillance Act (FISA), and as contrary to constitutional rights. But the defining characteristic of Plaintiffs' challenge is a complete lack of supporting evidence. Relying entirely on unsubstantiated allegations in their complaints, unverified media reports, and speculation, they allege that Government conduct for which they offer no proof has inflicted injury upon them for which they present no evidence.

In the wake of unauthorized disclosures about intelligence-gathering activities conducted by the NSA, the Government has acknowledged the existence and certain details of NSA counter-terrorism programs that appear to be implicated by Plaintiffs' allegations—although they bear no resemblance to the program of "mass surveillance" that Plaintiffs allege. First, under a provision of FISA known as Section 215, the 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. The Government does not collect, listen to, or record the content of any call under this program, nor does it collect the name, address, or financial information of any subscriber, customer, or party to a call. The program operates under FISC-imposed restrictions, 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. Specifically, 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, to create "comprehensive profiles" of ordinary Americans' lives as Plaintiffs speculate. As a result, only a tiny fraction of the collected metadata is ever reviewed, much less disseminated, by NSA analysts.

The NSA uses targeted electronic searches of these data, based on telephone numbers or other identifiers associated with foreign terrorist organizations, to 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 purposes has been authorized and periodically reauthorized over the past seven years under thirty-five separate orders issued by fifteen separate judges of the FISC. In two recent opinions (Exhibits A

and B, hereto),[1] the FISC concluded that the telephony metadata program is authorized by statute, and lawful under the Constitution.

Second, the Government has also publicly revealed certain information about its use of authority conferred by section 702 of the FISA, to collect, for foreign intelligence purposes, certain communications of non-U.S. persons located outside the United States, pursuant to approval of the FISC. This includes the collection now publicly referred to as "PRISM." Before authorizing collection under Section 702, the FISC must find that the Government has procedures in place (i) to ensure that only non-U.S persons abroad will be targeted, and (ii) to prevent the unwarranted retention or dissemination of information about U.S. persons (or their communications) that may be incidentally collected. NSA's retention and dissemination of communications thus acquired is governed by minimization procedures that the FISC has approved as consistent with FISA's requirements and the Fourth Amendment.

Finally, the Government has also declassified and officially acknowledged the existence of a FISC-authorized program involving collection and analysis, for foreign intelligence purposes, of non-content bulk Internet metadata (such as the "to" and "from" lines of an e-mail, and the date and time an e-mail was sent) carried out under the "pen register, trap and trace" provision of FISA. This program—which was discontinued in 2011—was conducted under FISC orders requiring the Government to comply with minimization procedures that prohibited access to the data except for purposes of queries using selection terms reasonably suspected of being associated with foreign terrorist organizations (as in the case of bulk telephony metadata).

---

[1] *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, BR 13-109, Amended Memorandum Opinion August 29, 2013 (Aug. 29 FISC Op.) (Exh. A, hereto); *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, BR 13-158, Memorandum, October 11, 2013 (Oct. 11 FISC Op.) (Exh. B, hereto).

Plaintiffs' motions for preliminary relief are based entirely on misconceptions and conjecture about the scope of these activities, and potential misuse of the information acquired. As a threshold matter, Plaintiffs offer no proof that any metadata about their communications, or the contents of their communications, have ever been collected by the NSA, much less exploited to expose intimate details about their personal lives and associations. That being the case, they can neither establish their standing to maintain these actions in the first place, nor make the showing of irreparable harm required to obtain preliminary injunctive relief.

Plaintiffs also fail to show any likelihood of success on the merits of their claims. Their contention that the Government's alleged conduct exceeds its statutory authority under FISA is precluded, *inter alia*, by FISA's detailed scheme for judicial review of specified intelligence activities. In any event, as the FISC has repeatedly (and twice recently) found, the Government's bulk collection of telephony metadata is lawful under FISA because there are reasonable grounds for believing that such data as a whole are relevant to authorized FBI counter-terrorism investigations. The FISC has similarly authorized the NSA's PRISM collection of non-U.S. person communications, and prior collection of bulk Internet metadata, as consistent with FISA.

Plaintiffs' Fourth Amendment challenge to the NSA's collection of communications metadata is foreclosed by the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), which held that there is no reasonable expectation of privacy in such non-content information. And as the FISC has held, the Government's procedures for collecting communications of non-U.S. persons located abroad under Section 702 also comport with Fourth Amendment requirements. Plaintiffs' First Amendment claim rests entirely on their hypothetical premise—inconsistent with FISC-imposed safeguards—that the Government uses the communications information it acquires to track their activities and interpersonal relationships. But no parallel can be drawn between the alleged intelligence-gathering activities Plaintiffs seek

to put at issue here and cases in which individuals or organizations were compelled to disclose personally identifying information, or membership lists, based on their protected associational activities. Plaintiffs cite no authority for their meritless due-process claim.

In sum, the NSA's collection of communications metadata, and of communications acquired by targeting foreign persons located abroad, are important tools in the Government's counter-terrorism arsenal, and are lawful. Unsubstantiated conjecture about how these programs 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' motions for preliminary injunctions should be denied.

STATEMENT OF FACTS

I. STATUTORY BACKGROUND

Congress enacted FISA to authorize and regulate certain governmental surveillance of communications and other activities for purposes of gathering foreign intelligence. In enacting FISA, Congress also created the FISC, an Article III court of 11 appointed U.S. district judges with authority to consider applications for and grant orders authorizing electronic surveillance and other forms of intelligence-gathering by the Government. 50 U.S.C. § 1803(a); *see In re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 486 (F.I.S.C. 2007).

Plaintiffs' various allegations implicate different provisions of FISA. First, FISA's "business records" provision, 50 U.S.C. § 1861, enacted by section 215 of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (Section 215), authorizes the FISC to issue an order for the "production of any tangible things (including books, records, papers, documents, and other items) for an investigation [1] to obtain foreign intelligence information not concerning a United States person or [2] to protect against international terrorism" (provided, in the case of a counter-terrorism investigation of a "United States person," that "such investigation . . . is not

conducted solely upon the basis of activities protected by the first amendment to the Constitution"). 50 U.S.C. § 1861(a)(1). The records must be of a type obtainable by either a grand jury subpoena, or an order issued by a U.S. court directing the production of records or tangible things. *Id*. § 1861(c)(2)(D).

The Government's application for an order under Section 215 must include, among other things, a statement of facts showing that there are "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism." *Id*. § 1861(b)(2)(A). The investigation must be authorized and conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor thereto). *Id*. § 1861(a)(2)(A), (b)(2)(A). Information acquired from the records or other tangible items received in response to a Section 215 order "concerning any United States person may be used and disclosed by [the Government] without the consent of [that] person only in accordance with . . . minimization procedures," adopted by the Attorney General and enumerated in the Government's application, that "minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the [Government's] need . . . to obtain, produce, and disseminate foreign intelligence information." *Id*. § 1861(b)(2)(B), (g)(2), (h). The FISC must find that these requirements have been met before it issues the requested order, which in turn must direct that the minimization procedures described in the application be followed. *Id*. § 1861(c)(1).

Section 215 includes a scheme providing for judicial review of a business records order once it is granted, but only in limited circumstances. Specifically, it allows "[a] person receiving a production order [to] challenge the legality of that order" by filing a petition with the "review pool" of FISC judges designated under 50 U.S.C. § 1803(e)(1) to review production orders under

Section 215. *Id*. § 1861(f)(1), (2)(A)(i). A "pool" judge considering a petition to modify or set aside a production order may grant the petition if the judge finds that the order does not meet the requirements of Section 215 or "is otherwise unlawful." *Id*. § 1861(f)(2)(B). Thus, a production order can be set aside if it exceeds the authority conferred by Section 215 or is unconstitutional. 1 D. Kris & J. Wilson, National Security Investigations & Prosecutions § 19:10 at 714 (2d ed. 2012) (Kris & Wilson). Either the Government or a recipient of a production order may appeal the decision of the pool judge to the FISC Court of Review, with review available thereafter on writ of certiorari in the Supreme Court. 50 U.S.C. § 1861(f)(3); *see id*. § 1803(b). Section 215's carefully circumscribed provisions for judicial review were added when Congress reauthorized the USA PATRIOT Act in 2006, and these provisions authorized contested litigation before the FISC for the first time. 1 Kris & Wilson § 5:5, 19:7 (2d ed. 2012). The FISA does not provide for review of Section 215 orders at the behest of third parties.

Plaintiffs' claims also appear to put at issue section 702 of the FISA, enacted by the FISA Amendments Act of 2008, Pub. L. 110-261, § 101(a)(2), 122 Stat. 2436, codified at 50 U.S.C. § 1881a (Section 702). Section 702 provides that the Attorney General and the Director of National Intelligence (DNI) may authorize jointly, for up to one year, the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." *Id*. § 1881a(a). The statute expressly stipulates that the Government "may not intentionally target any person known at the time of acquisition to be located in the United States," "may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States," and "may not intentionally target a United States person reasonably believed to be located outside the United States." *Id*. § 1881a(b). Like Section 215,

Section 702 provides a right of judicial review of a Section 702 directive to a recipient of a directive. *Id*. § 1881a(h)(4), (6).

Before the Attorney General and the DNI may authorize the targeting of foreign persons abroad under the statute, they must first obtain (absent exigent circumstances) a FISC order approving the authorization. *See id*. § 1881a(a) & (i)(3). Section 702 requires the FISC to find that the Government's targeting procedures are reasonably designed to ensure that only non-U.S. persons who are outside the United States will be targeted in any Section 702 acquisition. *See id*. § 1881a(e). To the extent that a Section 702 acquisition results in the incidental collection of information concerning U.S. persons (such as those, *e.g*., communicating with the target of the surveillance), Section 702 addresses that circumstance in the same fashion as the original FISA: it requires the application of FISC-approved minimization procedures designed to prevent the unwarranted retention or dissemination of such information. *See id*.

Finally, FISA's so-called "pen/trap" provision may also be implicated by Plaintiffs' claims regarding bulk collection of Internet metadata. Similar in structure to Section 215, the pen/trap statute authorizes the FISC, upon application by the Government, to issue an order "approving the installation and use of a pen register or trap and trace device," *see* 50 U.S.C. § 1841(2); 18 U.S.C. § 3127(3), (4), to obtain information relevant to authorized FBI counter-terrorism investigations. 50 U.S.C. § 1842(a)(1), (c)(2).

I. THE COLLECTION OF INFORMATION AUTHORIZED BY FISA

A. Collection of Bulk Telephony Metadata Under Section 215

Plaintiffs first challenge the NSA's collection and analysis of bulk telephony metadata to discover communications with and among unknown terrorist operatives. Under this program, the FBI obtains orders from the FISC pursuant to Section 215 directing certain telecommunications service providers to produce to the NSA on a daily basis electronic copies of "call detail records,

or 'telephony metadata,'" Oct. 11, FISC Mem., Primary Order at 3-4, created by the recipient providers for calls to, from, or wholly within the United States. The NSA then stores, (and in limited circumstances) queries, and analyzes the metadata for counter-terrorism purposes. Under the terms of the FISC's orders, the NSA'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 has renewed the program thirty-five times under orders issued by fifteen different FISC judges. Declaration of Teresa H. Shea (Shea Decl.) ¶¶ 13-14, 16-17, 20 (Exh. C, hereto); Declaration of Robert J. Holley (Holley Decl.) ¶¶ 3, 6 (Exh. D, hereto); Aug. 29 FISC Op. at 29; Oct. 11 FISC Mem. at 2-6; *see also In re Application of the FBI for an Order Requiring the Production of Tangible Things [etc.]*, Dkt. No. BR 13-80, Primary Order (F.I.S.C. Apr. 25, 2013) (Exhibit E, hereto) at 3-4, 17; *id*., Secondary Order (Exhibit F, hereto) at 1-2, 4.

Under the FISC's orders, telephony metadata is defined as "comprehensive communications routing information" including but not limited to "originating and terminating telephone number[s], International Mobile Subscriber Identity (IMSI) number[s], International Mobile Station Equipment Identity (IMEI) number[s], trunk identifier[s], telephone calling card numbers, and time and duration of call." Primary Order at 3 n.1. By the express terms of the FISC's orders, "[t]elephony metadata does not include the name, address, or financial information of a subscriber or customer." *Id*.; Secondary Order at 2. The data are numerical only. The FISC's orders do not allow the NSA to obtain the name, address, or financial information of a subscriber, customer, or any party to a call. Nor do they permit the Government, under this program, to listen to or record the contents of any telephone conversations. Shea Decl. ¶¶ 13, 15, 18; Holley Decl. ¶¶ 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; *see* 50 U.S.C. § 1861(a)(1), (b)(2)(A). 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. Holley Decl. ¶ 10. FISC orders authorizing the NSA's collection of the metadata are in turn predicated on findings by the Court that there are "reasonable grounds to believe that the [records] sought are relevant to authorized investigations . . . being conducted by the FBI . . . to protect against terrorism." *See* Primary Order at 1-2; Aug. 29 FISC Op. at 28.

As also required by Section 215, the FISC's orders direct the Government to comply with "minimization procedures" that strictly limit access to and review of the metadata, and limit dissemination of information derived from the data, to valid counter-terrorism purposes. *See* 50 U.S.C. § 1861(b)(2)(B), (g), (h); Primary Order at 4-17; Holley Decl. ¶ 8; Shea Decl. ¶¶ 29-35. Under these restrictions, NSA analysts may access the metadata only for purposes of obtaining foreign intelligence information, and may do so only through "contact-chaining" queries (electronic 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 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 a selection term used to query the database is associated with one or more foreign terrorist organizations previously identified to and approved for targeting by the FISC. 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 finite periods of time. Shea Decl. ¶¶ 19-23, 31; Primary Order at 6-9. 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. Shea Decl. ¶¶ 20, 23.

Also under the FISC's orders, the accessible results of an approved query 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 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.

The NSA's 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 the NSA to use the database to conduct a level of historical analysis, and to discover contact links, that cannot practically be accomplished through targeted intelligence-gathering authorities. 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 is possible because the bulk collection of telephony metadata under the program 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.

Plaintiffs speculate that metadata collected under the program is being used to compile "rich comprehensive profile[s]" of every citizen, including "intimate details" about their lives and personal associations, *see* Pls.' Mem. in Supp. of their Mot. for Prelim. Inj., No. 13-cv-0851, ECF No. 13-1 (*Klayman I* Br.), at 11, but these anxieties are unfounded. Under the FISC's orders, the data may be queried, and the results may be shared, only to allow Government investigators to discover persons, including persons (and their associates) located in the United States, who have been in contact with known or suspected terrorist organizations, *see* Primary Order at 4, and may themselves be engaged in terrorist activity. The NSA does not use the data to provide the FBI with profiles on suspected terrorists (or anyone else), 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. Rather, it 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.

In addition to these, the NSA's activities under the FISC's orders are subject to an extensive regime of internal reporting, audits, and oversight; regular consultation with the NSA Office of the Inspector General, and the Department of Justice, to assess compliance with FISC orders; and monthly reports to the FISC including, *inter alia*, a discussion of NSA's application

of the "reasonable, articulable suspicion" standard and the number of times that query results containing U.S. person information have been shared with anyone outside NSA. *Id*. at 4-16.[2]

The Government has recently made public (and Plaintiffs have pointed to) 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 suspending the Government's authority to query the database without the court's approval) reauthorized the program in its current form.[3] Shea Decl. ¶¶ 36-43.

B. Targeted Collection of Communications Content Pursuant to Section 702

Plaintiffs' allegations also appear to put at issue the targeted collection of electronic communications under Section 702 of the FISAunder the PRISM collection. Although Plaintiffs offer no evidence to support their allegations about this program, the Government has acknowledged the following facts concerning this activity: Section 702 facilitates the targeted acquisition of foreign intelligence information concerning foreign targets located outside the United States under court oversight. Electronic communication service providers supply information to the Government pursuant to authorized directives issued by the Attorney General and the DNI. ODNI Fact Sheet at 1 (June 8, 2013) (Exh. G, hereto); *see* 50 U.S.C. §

[2] FISA also requires the Government to report to Congress regarding the use of its Section 215 authority, including copies of significant FISC orders and the Government's supporting pleadings. 50 U.S.C. §§ 1862, 1871.

[3] Among the most serious compliance problems was 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).

1881a(h)(1). Once targeted surveillance under Section 702 has been authorized, the NSA takes the lead in tasking relevant telephone and electronic communications selectors to target specific non-US persons reasonably believed to be located outside the United States. IC's Collection Programs Under Title VII of the FISA, at 3 (Exh. H, hereto). Consistent with the statute, the NSA's targeting procedures require that there be an appropriate, documented foreign intelligence purpose for the acquisition (such as for the prevention of terrorism, hostile cyber activities, or nuclear proliferation) and that the selector be used by a non-U.S. person reasonably believed to be located outside the United States. *Id.*; ODNI Fact Sheet at 1.

Once a target has been approved, the NSA uses two means to acquire the target's electronic communications. First, it acquires such communications directly from U.S.-based providers. This has been publicly referred to as the NSA's PRISM collection. Second, in addition to collection directly from providers, the NSA collects electronic communications as they transit internet "backbone" facilities within the United States. This is known as "upstream" collection. *See* IC's Collection Programs Under Title VII of the FISA, at 3-4; Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *9 & n.24.

Acquired communications are routed to the NSA, and the NSA can designate communications from specified selectors acquired through PRISM collection to be dual-routed to other intelligence agencies. Each agency that receives the collection has its own FISC-approved minimization procedures and may retain and disseminate communications acquired under Section 702 only in accordance with those procedures. In general, before an agency may disseminate information identifying a U.S. person, the information must reasonably appear to be foreign intelligence or evidence of a crime, or necessary to understand or assess foreign intelligence information. IC's Collection Programs Under Title VII of the FISA at 4. The FISC has approved the NSA's minimization procedures for collections under Section 702. *See* Aug.

24, 2012 FISC Op., 2012 WL 9189263, at *2-3; Nov. 30, 2011 FISC Op., 2011 WL 10947772; Oct. 3, 2011 FISC Op., 2011 WL 10945618.[4] Finally, the NSA's Section 702 collection activities are subject to extensive oversight by all three branches of the Government. ODNI Fact Sheet at 1-3; IC's Collection Programs Under Title VII of the FISA at 4-5.

C. Bulk Collection of Internet Metadata

Plaintiffs have also alleged unlawful collection by the Government of bulk Internet metadata. In addition to recent official declassification of the existence of the FISC-authorized collection of bulk telephony metadata under Section 215, the Government has also recently declassified the existence of FISC-authorized bulk collection of Internet metadata—that is, certain routing, addressing, and signaling information about Internet-based electronic communications such as e-mail. As explained in a recently released report to Congress, the Government at one time acquired bulk Internet metadata under orders issued by the FISC pursuant to FISA's pen/trap provision. *See* Report on the [NSA's] Bulk Collection Programs for USA PATRIOT Act Reauthorization (Exh. I, hereto) at 3.[5] The data collected included certain routing, addressing, and signaling information such as "'to' and 'from' lines in an e-mail . . . and the date and time an e-mail [was] sent," but not "the content of [an] e-mail [or] the 'subject' line." *Id*. at 3. NSA collected large amounts of this transactional information from certain telecommunications service providers and analyzed it to obtain foreign intelligence information.

[4] In an opinion issued on October 3, 2011, the FISC found the NSA's minimization procedures as applied to one aspect of the proposed collection—NSA's upstream collection of internet transactions containing multiple communications, or "MCTs"—deficient. Oct. 3, 2011 FISC Op., 2011 WL 10945618. The FISC subsequently determined that the NSA adequately remedied the deficiencies such that the procedures met the applicable statutory and constitutional requirements, and allowed the collection to continue. Aug. 24, 2012 FISC Op., 2012 WL 9189263, at *2-3; Nov. 30, 2011 FISC Op., 2011 WL 10947772. *See also* IC's Collection Programs Under Title VII of the FISA at 5.

[5] This 2011 report, and a similar briefing paper in 2009, were provided by the Department of Justice to the Senate and House Intelligence Committees. *See infra* at 38 & n.23.

Id. at 2. The FISC's orders authorizing this collection required the Government to comply with "minimization procedures" limiting the retention and dissemination of the metadata, including a requirement of "reasonable articulable suspicion" that selection terms used to query the bulk data were associated with foreign terrorist organizations. *Id*. at 3. This program of bulk Internet metadata collection was terminated in 2011, for operational and resource reasons. Letter from James R. Clapper to the Hon. Ron Wyden (July 25, 2013) (Exh. J, hereto), at 3.

III. PLAINTIFFS' ASSERTIONS IN THEIR PRELIMINARY INJUNCTION MOTIONS

According to Plaintiffs' submissions, Plaintiff Larry Klayman is an attorney and the founder, chairman, and general counsel of Freedom Watch, a public interest organization engaged in political activism. *See Klayman I* Br. at 12. He and his co-Plaintiffs, Charles and Mary Ann Strange, who are the parents of a U.S. Navy Seal Team Six member killed in Afghanistan in 2011, *id*. at 14, allege that a "secret and illicit government scheme" of "mass surveillance" "systematically gather[s], intercept[s] and analyze[s] vast quantities of telephonic and online 'metadata' of U.S. citizens," Pls.' Mem. in Supp. of their Mot. for Prelim. Inj., No. 13-cv-0881, ECF No. 10-1 (*Klayman II* Br.), at 1, and that electronic communications service providers have given the NSA "blanket access to [their] vast databases," *id*. at 3, so "the government collects and stores every internet communication made through the major online services . . . ." *Id*. at 27.[6] Plaintiffs alleged that the NSA is using this information "to build

[6] Almost all of Plaintiffs' assertions about the nature and extent of the challenged programs are based on unsubstantiated allegations in their complaints or unverified online media reports. Such evidence is insufficient to support the issuance of a preliminary injunction. *See In re Akers*, 487 B.R. 326, 331 (D.D.C. 2012) (denying preliminary injunction motion that "only set[ ] forth insufficient conclusory assertions of wrong"); *Miniter v. Moon*, 684 F. Supp. 2d 13, 16 (D.D.C. 2010) ("As the plaintiff has offered *no* evidence from which the court could assess the merits of his arguments, he has failed to demonstrate a likelihood of success on the merits of his claim."). This is especially true to the extent that Plaintiffs seek to rely on these sources to support allegations about the scope and conduct of classified intelligence-gathering activities.

comprehensive profiles of ordinary Americans," including their "personal associations" and "extremely sensitive details" about them. *Id*. at 2. Plaintiffs also claim that "it is logical to conclude that Plaintiff Klayman is subjected to excessive and intrusive surveillance and monitoring by the NSA," in order to "coerce" and "intimidate" him "into silence," because "it is indisputable that [he] has become the prime target of the NSA." *Klayman I* Br. at 13.

Plaintiffs contend that the NSA's alleged' "illegal surveillance directly impacts [their] ability to communicate via telephone, email, and otherwise, out of fear" that their confidential and private "communications will be overheard or obtained by the NSA's surveillance program." *Id*. at 14, 15. They argue that bulk collection of telephony metadata—which has been found to be lawful thirty-five times by fifteen different Article III judges on the FISC—exceeds the authority conferred by Section 215, *see id*. at 17-19, and violates the First, Fourth, and Fifth Amendments. *See id*. at 19-27. Plaintiffs also argue that the "PRISM program," and bulk collection of Internet metadata, violates the same provisions of the Constitution, *Klayman II* Br. at 30, and exceeds statutory authority under Section 215, *see id*. at 5, 19-20, even though the authority for those programs lies under Section 702 and the pen/trap provision, respectively.

Plaintiffs seek preliminary injunctions (1) enjoining these FISC-authorized activities (2) requiring the NSA to "purge" all of Plaintiffs' collected metadata, if any, and (3) prohibiting the NSA from querying the metadata using identifiers associated with Plaintiffs. *See Klayman I* Br. at 4, 30-31; *Klayman II* Br. at 4-5, 32-33.

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).

Media speculation about the Government's sources and methods of acquiring intelligence cannot be equated with official release or acknowledgment of such information. *See Afshar v. Department of State*, 702 F.2d 1125, 1130-31 (D.C. Cir. 1983)

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); *In re Navy Chaplaincy*, 697 F.3d 1171, 1178 (D.C. Cir. 2012). "A positive showing on all four factors is required." *Bayer HealthCare, LLC v. FDA*, __ F. Supp. 2d __, 2013 WL 1777481, *5 (D.D.C. Apr. 17, 2013).[7] 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 a "somewhat higher" demonstration of entitlement to preliminary relief than is normally required. *See Paleteria La Michoacana, Inc. v. Prods.Lacteos Tocumbo S.A. de C.V.*, 901 F. Supp. 2d 54, 56 (D.D.C. 2012); *Sierra Club v. Johnson*, 374 F. Supp. 2d 30, 33 (D.D.C. 2005).

Further, a preliminary injunction cannot issue on the mere basis of speculation. *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 Sherley v. Sebelius*, 644 F.3d 388, 392-93 (D.C. Cir. 2011). Finally, a court deciding a preliminary injunction motion "must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief," *Winter*, 555 U.S.

[7] While Plaintiffs assume that a "continuum" or "sliding scale" approach applies here with respect to these four factors, *Klayman I* Br. at 17; *Klayman II* Br. at 19 (citing *CityFed Fin. Corp. v. OTS*, 58 F.3d 738, 747 (D.C. Cir. 1995)), they overlook that the decision they cite in support of this proposition preceded the Supreme Court's decision in *Winter*, and that the "continued viability" of the sliding scale approach in all cases post-*Winter* has been called into question by the D.C. Circuit and this court. *Sherley v. Sebelius*, 644 F.3d 388, 392-93 (D.C. Cir. 2011); *Jack's Canoes & Kayaks, LLC v. Nat'l Park Serv.*, 933 F. Supp. 2d 58, 76 (D.D.C. 2013).

at 24 (internal quotations omitted), and "should pay particular regard for the public consequences in employing the extraordinary remedy of injunction." *Id*. (internal quotations omitted).

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

Plaintiffs' request for preliminary injunctive relief must be denied because they have not alleged injuries sufficient to sustain Article III standing, a jurisdictional defect in their case that precludes any likelihood of success on their claims. Likewise, Plaintiffs have not shown that they will suffer any irreparable harm absent an injunction, an equally insuperable bar to relief.

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

"The judicial power of the United States" is limited by Article III of the Constitution "to the resolution of 'cases' and 'controversies'," *Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464, 471 (1982), and a demonstration of a plaintiff's standing to sue "is an essential and unchanging part of the case-or-controversy requirement," *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). Standing is also usually the "first component of the likelihood of success on the merits prong," *Jack's Canoes & Kayaks*, 933 F. Supp. 2d at 76 (quotations omitted), because Plaintiffs "must have standing" for "this Court to have subject matter jurisdiction over" their "motion[s] for a preliminary injunction." *Dominquez v. Dist. of Columbia*, 536 F. Supp. 2d 18, 23-24 (D.D.C. 2008) (Leon, J.). The standing inquiry "has been especially rigorous when reaching the merits of the dispute would force [a court] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013) (internal quotations omitted). The Supreme Court has also "often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs." *Id*.

To establish Article III standing, Plaintiffs must show that they have suffered injury in fact, "an invasion of a legally protected interest," *Lujan*, 504 U.S. at 560, that is "concrete, particularized, and actual or imminent." *Amnesty Int'l USA*, 133 S. Ct. at 1147. A "threatened injury must be *certainly* impending to constitute injury in fact," whereas "allegations of *possible* future injury are not sufficient." *Id*. The alleged injury must also be "fairly traceable to the challenged action" and be "redressable by a favorable ruling." *Monsanto Co. v. Geertson Seed Farms*, 130 S. Ct. 2743, 2752 (2010). Because Plaintiffs must show that they have standing "with the manner and degree of evidence required at the successive stages of the litigation," *Lujan*, 504 U.S. at 561, Plaintiffs cannot now rely on mere allegations but must come forth with evidence to support their standing in order to obtain preliminary injunctive relief. *See Doe v. Rumsfeld*, 297 F. Supp. 2d 119, 130 (D.D.C. 2003).

Plaintiffs have failed to adduce specific facts demonstrating that they have standing to challenge any of the intelligence-gathering activities they allege. Plaintiffs Larry Klayman and Charles Strange attest that they have for many years been subscribers of cellular telephone service provided by Verizon Wireless, and users of Internet services offered by a variety of electronic communications service providers "at all material times." Affidavit of Larry Klayman (Klayman Aff.) ¶ 3, ECF No. 13-2; Affidavit of Charles Strange (Strange Aff.) ¶¶ 2-3, ECF No. 13-3. They state that the alleged collection of information about (and contained in) their telephonic and electronic communications "impact[s]" their ability to communicate by telephone, e-mail, and other means due to their "concern" that these communications will be "overheard" or "obtained" by the NSA and "used against" them in some manner. Klayman Aff. ¶ 10; Strange Aff. ¶ 11. On the strength of these assertions, Plaintiffs claim to have standing to challenge the legality of the Government's (1) bulk collection of telephony metadata, (2) alleged "mass" collection of the contents of U.S.-person communications, and (3) alleged bulk collection

of Internet metadata. *See Klayman I* Br. at 9-12; *Klayman II* Br. at 13, 15. In fact, Plaintiffs have not demonstrated that they have suffered injury traceable to any of these activities.

Plaintiffs have not asserted sufficient facts to show that any information about or contained in their telephonic or Internet-based communications has been or imminently will be collected under any of these alleged programs. With regard to bulk telephony metadata, although Plaintiffs Klayman and Strange assert that they are or have been subscribers and users of cellular telephone service provided by "Verizon Wireless," Klayman Aff. ¶ 3; Strange Aff. ¶ 2, they offer no proof that the Government has ever collected bulk telephony metadata from that company. And although the Government has acknowledged that the telephony metadata program remains ongoing, and that multiple telecommunications service providers have been participants in the program since its inception in 2006, *see supra* at 9, 11-12, the Government has not officially disclosed the identities of the group of providers from which bulk telephony metadata are collected. Plaintiffs' assertion that they are Verizon Wireless customers does not establish that the NSA has collected telephony metadata regarding their communications.[9]

With respect to NSA's alleged "PRISM" collection of communications under Section 702, the Government has acknowledged that, for foreign intelligence purposes, the NSA targets non-U.S. persons, located outside the United States, by acquiring communications directly from

[9] The Government has acknowledged the authenticity of an unlawfully disclosed Secondary Order of the FISC dated April 25, 2013, which listed Verizon Business Network Services, Inc. (VBNS) as a recipient of that order at that time. VBNS, however, is a separate business entity from Verizon Wireless. *See United States ex rel Shea v. Verizon Bus. Network Servs., Inc.*, 904 F. Supp. 2d 28, 30 (D.D.C. 2012). Except for this single order of April 2013, the Government has not declassified any further information regarding VBNS's participation in this program or that of any other provider. In any event, at this stage of proceedings, Plaintiffs' allegations do not indicate that they were subscribers of VBNS or that Verizon Wireless is subject to Section 215 collection. Plaintiffs protest that "the facts, information, documents, and evidence" pertinent to their claims "are uniquely in the hands of Defendants," *Klayman I* Br. at 31, but as the Supreme Court pointedly observed in *Amnesty International*, it is Plaintiffs' "burden to prove their standing by pointing to specific facts, not the Government's burden to disprove standing by revealing details of its surveillance" programs. 133 S. Ct. at 1149 n.4

certain U.S.-based electronic communications service providers. This activity is conducted pursuant to authority conferred by and (approval obtained from) the FISC under Section 702. *See supra* at 13-15; Oct. 3, 2011 WL 10945618, at *9 & n.24. Although Plaintiffs have asserted that they are users of Internet-based communications services offered by a number of U.S.-based providers, *see* Klayman Aff. ¶ 3; Strange Aff. ¶ 3, their affidavits contain no evidence that the NSA actually has targeted communications of theirs (or of any non-U.S. persons with whom they communicate) for foreign intelligence purposes authorized under Section 702. Nor do they allege that communications of theirs have been or will be acquired incidental to the targeting of non-U.S. persons under Section 702. *See* Oct. 3, 2011 WL 10945618, at 5. Rather, they simply speculate that their communications have been intercepted based on their level of political activism, *see, e.g.*, Klayman Aff. ¶¶ 4-8, 12, or assume that is so based on their allegations of "mass surveillance" of the contents of Americans' electronic communications, allegations for which they offer no proof whatsoever. *See Klayman II* Br. at 3, 12, 27.[10]

With regard to bulk Internet metadata, the Government has declassified the existence of a program under which the NSA obtained such data pursuant to court orders issued by the FISC, but that the program ceased in 2011, *see supra* at 16, and the Government has not disclosed the scope on which it operated. Plaintiffs offer no proof that the NSA has actually acquired Internet metadata about their communications, or continues to do so. *See* Klayman Aff. ¶¶3, 10; Strange Aff. ¶¶ 3, 4, 11, 18-19.

[10] Plaintiffs assert in their briefs that "it is logical to conclude that Plaintiff Klayman is subjected to excessive and intrusive surveillance and monitoring by the NSA. In fact, it is indisputable that [he] has become the prime target of the NSA . . . ." *Klayman I* Br. at 13; *Klayman II* Br. at 14. These conclusory and unsubstantiated arguments of counsel, and others like them in Plaintiffs' legal memoranda, are not evidence of injury on which they can base their standing. *Conservation Force v. Salazar*, 715 F. Supp. 2d 99, 106 n.9 (D.D.C. 2010).

Given that Plaintiffs fail to establish that any information about their communications (whether metadata or content) has been or will be collected, their stated "concern" that communications of theirs "will be overheard or obtained by" NSA, Klayman Aff. ¶ 10; Strange Aff. ¶ 11, is speculative and does not constitute injury-in-fact. *See Amnesty Int'l USA*, 133 S. Ct. at 1148-50. In *Amnesty International*, various individuals and organizations challenged the constitutionality of Section 702, which expanded the Government's authority to intercept the communications of non-U.S. persons located abroad. *See id*. at 1144. They alleged, similar to Plaintiffs here, that there was an "objectively reasonable likelihood that their communications [would] be acquired . . . at some point in the future," based on claims that they maintained regular contact with persons whose communications they believed would be targeted for acquisition by the Government. *Id*. at 1145-46. The Supreme Court found that this "threatened injury" was not "certainly impending" and so did not constitute an injury in fact, because it "was speculative whether the Government [would] imminently target communications to which [they would be] parties." *Id*. at 1148. The same is true, indeed, all the more so here. As the foregoing discussion reveals, Plaintiffs fail to show that NSA collection of information about or contained in their communications has ever occurred, or is "certainly impending."[11]

In addition, given that Plaintiffs have not established that their communications, or metadata about their communications, either have been or imminently will be subject to collection under any of the challenged NSA programs, their assertions that these programs have

[11] Nor do any of the incidents that Plaintiff Strange labels "technological abnormal intrusions," Strange Aff. ¶¶ 12-17; Klayman Aff. ¶ 11, support a finding that Plaintiffs' telephony or Internet-based communications were collected by the NSA. The incidents that Plaintiffs describe—unexplained text messages, a "hoax" e-mail, and a widely publicized computer virus scam, *see* FBI: New Internet Scam (Aug. 2012), www.fbi.gov/news/stories/2012/august/new-internet-scam; Citadel Malware Continues to Deliver Ransomware in Attempts to Extort Money (Aug. 9, 2012), www.ic3.gov/media/2012/120809.aspx-- bear no resemblance to the alleged NSA data-collection activities, and Plaintiffs point to no evidence linking these incidents to the NSA, or any other Government agency.

"directly and significantly impacted" their "ability to communicate via telephone, e-mail, or otherwise," and to engage in public advocacy, Klayman Aff. ¶¶ 9-10; Strange Aff. ¶¶ 11, 19-20, reflect only subjective fears on their part, fears that are insufficient to establish a cognizable injury for purposes of standing. *Amnesty Int'l USA*, 133 S. Ct. at 1152 (holding that the costs allegedly incurred in efforts to avoid possible surveillance was the "product of" the plaintiffs' "fear of surveillance" and that "such fear is insufficient to create standing"); *Laird v. Tatum*, 408 U.S. 1, 10, 14 (1972) (holding that "[a]llegations of a subjective 'chill'" arising from plaintiffs' knowledge of the existence of "a governmental investigative and data-gathering activity," without "any specific action of the [Government] against them," were "not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm"); *United Presbyterian Church in the USA v. Reagan*, 738 F.2d 1375, 1378 (D.C. Cir. 1984) (chilling effect produced by fear of surveillance is an sufficient basis for standing under *Laird*).[12]

For these reasons, Plaintiffs have not shown a clear or substantial likelihood of success on their claims because they have not established their standing.

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

To satisfy the "high standard" for showing irreparable harm, *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 297 (D.C. Cir. 2006), which is "perhaps the single most important prerequisite for the issuance of a preliminary injunction," *Stand Up for California! v. U.S. Dep't of the Interior*, 919 F. Supp. 2d 51, 81 (D.D.C. 2013) (internal quotations omitted),

[12] In their brief, Plaintiffs also assert that the challenged programs "undoubtedly will dissuade, and has dissuaded, potential clients, whistleblowers, and others from contacting Plaintiff Klayman . . . ." *Klayman II* Br. at 16. Even setting aside that the arguments of counsel in legal memoranda are not evidence, *Conservation Force*, 715 F. Supp. 2d at 106 n.9, this assertion would not otherwise "establish injury that is fairly traceable to" the challenged NSA programs because it rests on speculation about unidentified third parties' own speculative "fear[s] of surveillance." *Amnesty Int'l USA*, 133 S. Ct. at 1152 n.7; *see also Lujan*, 504 U.S. at 562 (plaintiffs have the burden of "showing that [the] choices [of third-parties] have been or will be made in such manner as to produce causation and permit redressability of injury.").

Plaintiffs must show that their asserted injuries are "certain" and "great," rather than "theoretical," and "of such *imminence* that there is a 'clear and present' need for equitable relief" to prevent this harm that would otherwise be "beyond remediation." *Id*. (internal quotations omitted). For the same reasons that Plaintiffs failed to demonstrate that they suffered a sufficiently concrete injury to establish standing, they have failed to produce competent evidence showing that they are "likely to suffer irreparable harm before a decision on the merits can be rendered." *Id*. (internal quotations omitted).

Further exposing Plaintiffs' lack of irreparable harm is their four-month delay in filing their preliminary injunction motions. *See Gordon v. Holder*, 632 F.3d 722, 725 (D.C. Cir. 2011); *see also Fund for Animals v. Frizzel*, 530 F.2d 982, 987 (D.C. Cir. 1975) (denying preliminary injunctive relief and noting that a delay of forty-four days after final regulations were issued was "inexcusable"); *Brown v. Dist. of Columbia*, 888 F. Supp. 2d 28, 33 (D.D.C. 2012) (Leon, J.) (finding that the plaintiff's six-month delay in seeking injunctive relief "directly undercuts any argument that her injury is of such imminence that there is a clear and present need for equitable relief to prevent irreparable harm") (internal quotations omitted). Here, Plaintiffs filed their Complaints against the Government Defendants in these cases on June 6 (*Klayman I*, Dkt. No. 1) and June 12, 2013 (*Klayman II*, Dkt. No. 1), but then inexplicably waited over four months, until October 29, to seek preliminary injunctive relief. *See* Klayman I, Dkt. No. 13; Klayman II, Dkt. No. 10. This is yet another reason why this Court "should be reluctant to award relief." *NRDC v. Pena*, 147 F.3d 1012, 1026 (D.C. Cir. 1998).

II. PLAINTIFFS' CLAIM THAT THE ALLEGED NSA ACTIVITIES EXCEED STATUTORY AUTHORITY IS PRECLUDED BY STATUTE

Plaintiffs' requests for preliminary injunctions must also be denied because they have not shown a likelihood of success on the merits of any of their claims.

As an initial matter, neither of Plaintiffs' complaints even purports to state a claim against the Government Defendants that the alleged NSA collection of information about their communications exceeds statutory authority. The only statutory claims in *Klayman I* are directed against Verizon and its Chief Executive Officer Lowell McAdam (Sixth and Seventh Claims for Relief). The complaint in *Klayman II* contains two claims for "Divulgence of Communications Records in Violation of 18 U.S.C. §§ 2702(a)(1) and/or (a)(2)" that purport to be against "Each and Every Defendant" (Sixth and Seventh Claims for Relief).[13] Plaintiffs allege that those claims are brought pursuant to 18 U.S.C. § 2707, which they claim "provides a civil action for any person aggrieved by knowing or intentional violation of 18 U.S.C. § 2702," (*Klayman II* Compl. ¶¶ 108, 115). 18 U.S.C. § 2707, however, expressly excludes the United States from the cause of action. 18 U.S.C. § 2707(a) ("Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, *other than the United States*, which engaged in that violation such relief as may be appropriate.") (emphasis added). 18 U.S.C. § 2712 provides for a cause of action against the United States for certain violations, but (1) Plaintiffs have not alleged a claim under this statute, (2) this statute only provides for money damages, not injunctive relief, and (3) this statute contains an exhaustion requirement that Plaintiffs have not satisfied. 18 U.S.C. § 2712(b).

To the extent Plaintiffs might seek to rely on the Administrative Procedure Act (APA), 5 U.S.C. § 706, for a cause of action for injunctive relief against the United States for alleged violations of 18 U.S.C. § 2702(a)(1), (2) (although it is not pled), such a claim would be

[13] 18 U.S.C. § 2702(a)(1) and (a)(2) relate to the divulgence of the contents of communications, as opposed to communication records.

impliedly precluded by Congress through its establishment of a cause of action for money damages only in 18 U.S.C. § 2712. In *Jewel v. NSA*, 2013 WL 3829405, at *12 (N.D. Cal. July 23, 2013), the court held that by excluding the United States from 18 U.S.C. § 2707, which provides for injunctive relief, and only authorizing a cause of action for money damages against the United States in § 2712, Congress intended to forbid injunctive and declaratory relief against the United States under the Stored Communications Act (18 U.S.C. § 2701, *et seq*.).

As a general matter, APA section 702 waives sovereign immunity for actions against the Government "seeking relief other than money damages." It is subject to a number of significant exceptions, however, two of which apply here. First, section 702 itself provides that "[n]othing herein . . . confers authority to grant relief if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought." 5 U.S.C. § 702. Second, mirroring the first exception, the APA provides that its chapter on judicial review, including section 702, does not apply "to the extent that . . . statutes preclude judicial review." *Id*. § 701(a)(1).

The first exception "prevents plaintiffs from exploiting the APA's waiver to evade limitations on suit contained in other statutes." *Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak*, 132 S. Ct. 2199, 2204-05 (2012). As Congress explained when it enacted the APA's waiver of immunity, this "important carve-out," *id*. at 2204, makes clear that Section 702 was "not intended to permit suit in circumstances where statutes forbid or limit the relief sought," that is, where "Congress has consented to suit and the remedy provided is intended to be the exclusive remedy." H.R. Rep. No. 94-1656, at 12-13 (1976), 1976 WL 14066, *12-13. "For example, . . . a statute granting the United States' consent to suit, i.e., the Tucker Act, 'impliedly forbids' relief other than the [damages] remedy provided by the Act." *Id*. Thus, "'when Congress has dealt in particularity with a claim and [has] intended a specified remedy'—including its exceptions—to be exclusive, that is the end of the matter; the APA does not undo

the judgment." *Pottawatomi Indians*, 132 S. Ct. at 2205 (quoting *Block v. North Dakota ex rel. Bd. of Univ. and Sch. Lands*, 461 U.S. 273, 286 n. 22 (1983)).

To much the same effect, section 701(a)(1) of the APA withdraws section 702's waiver of immunity where "statutes preclude judicial review." 5 U.S.C. § 701(a)(1) ("This chapter applies, according to the provisions thereof, except to the extent that (1) statutes preclude judicial review"). "Whether and to what extent a particular statute precludes judicial review is determined not only from its express language, but also from the structure of the statutory scheme, its objectives, its legislative history, and the nature of the administrative action involved." *Block v. Cmty. Nutrition Inst.*, 467 U.S. 340, 349 (1984). "[W]hen a statute provides a detailed mechanism for judicial consideration of particular issues at the behest of particular persons, judicial review of those issues at the behest of other persons may be found to be impliedly precluded." *Id.*; *see Pottawatomi Indians*, 132 S. Ct. at 2208.

Congress evidenced its intent that persons such as Plaintiffs, who claim to be subscribers and users of electronic communications services, not be permitted to challenge the statutory basis of orders to produce electronic communications or communications records, by explicitly providing a right of judicial review only to the recipients of such orders. Congress specifically authorized challenges to Section 215 production orders only by recipients of those orders—the entities that create and own the records—and permitted those entities to challenge production orders only by filing a challenge in the FISC. 50 U.S.C. § 1861(f)(2)(A)(i), (B). The purpose of this provision was to "place Section 215 proceedings on a par with grand jury proceedings, where the subpoena recipient obviously knows of its existence and can challenge it in court." *Implementation of the USA PATRIOT Act: Hearing Before the H. Subcomm. on Crime, Terrorism, and Homeland Security, Comm. on the Judiciary*, 109th Cong. at 65 (2005)

(statement of Robert Khuzami). Congress recognized, however, that allowing a similar right of action by third parties would be incompatible with the secrecy required for Section 215 orders.[14]

To promote its effective functioning as a tool for counter-terrorism, Section 215, like other provisions of FISA, establishes a secret and expeditious process that involves only the Government and the recipient of the order. *See* 50 U.S.C. § 1861(d)(1) (recipient may not "disclose to any other person that the [FBI] has sought or obtained" an order under Section 215). Under the statutory framework, third parties such as Plaintiffs, who are not recipients of Section 215 orders, are not even supposed to know of their existence, nor play a role in the process of testing their compliance with the statute. *See, e.g.*, H.R. Rep. No. 109-174 at 128 (2005). The fact that Plaintiffs learned about the telephony metadata program order as the result of an unauthorized and unlawful disclosure does not change this essential facet of FISA's structure. Allowing third parties to contest an order's compliance with Section 215's relevance and other requirements would potentially compromise the secrecy and efficiency of the process that Congress envisioned.

Were there any doubt, Congress provided expressly that a Section 215 order "shall remain in effect" unless it has been "explicitly modified or set aside consistent with this subsection." 50 U.S.C. § 1861(f)(2)(D). Thus, Congress clearly limited the right to contest the legality of Section 215 production orders to recipients of such orders who file petitions for review with the FISC. This "detailed mechanism for judicial consideration of particular issues" under Section 215 "at the behest of particular persons" means that "judicial review of those

[14] *See id*. ("Beyond this amendment, however, the confidentiality provisions of Section 215 should not be disturbed. You do not want potential terrorists to know you are investigating them or are aware of their plans."). *See also* H.R. Rep. No. 109-174 at 128 (right to challenge Section 215 order can only be given to the recipient, not the target, because the target does not know about it); *id*. at 268 (statutory prohibition on disclosing Section 215 order to subject prevents the subject from challenging it).

issues at the behest of other persons" is "impliedly precluded." *Cmty. Nutrition Inst.*, 467 U.S. at 349 (holding that statutory scheme allowing dairy handlers to seek review of milk market orders precluded actions by consumers); *see also Ark. Dairy Co-op Assn., Inc. v. USDA*, 573 F.3d 815, 822-23 (D.C. Cir. 2009) (dairy producers, who like handlers are given a role in the regulatory process, could also challenge milk market order); *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 128-29 (E.D. Va. 2011) (provision of Stored Communications Act allowing Twitter subscribers to challenge orders requiring production to Government of "backup information" impliedly prohibited statutory challenge by subscribers to order requiring production of electronic records pertaining to them).[15]

18 U.S.C. § 2712 also expresses Congress' intent to preclude a statutory claim under Section 215 by Plaintiffs. 18 U.S.C. § 2712 creates a damages action against the Government for violations of three specified provisions of FISA but omits Section 215 from that list, and provides no action for prospective relief. 18 U.S.C. § 2712(a). The three specified provisions of FISA are sections 106(a), 305(a), and 405(a), which respectively impose restrictions on the use and disclosure of information obtained from electronic surveillance, physical searches, and pen registers or trap and trace devices authorized under FISA. *See* 50 U.S.C. §§ 1806(a), 1825(a), 1845(a).[16] Significantly, violations of the parallel "use" provision of Section 215, 50 U.S.C. § 1861(h), which restricts the Government's use and disclosure of tangible things received in

[15] Like Section 215, Section 702 of FISA, under which PRISM collection occurs, provides that an electronic communications service provider who receives a directive under Section 702 may challenge its lawfulness before the FISC. 50 U.S.C. § 1881a(h)(4), (6). *See also Amnesty Int'l*, 133 S. Ct. at 1154. Thus, any claim by Plaintiffs that the NSA exceeded its statutory authority in collecting their communications under PRISM—should it survive the significant standing problems discussed above—would be impliedly precluded as well.

[16] As explained above, even if the complaints did plead a violation of 50 U.S.C. § 1845(a), 18 U.S.C. § 2712 only provides a damages remedy for such a violation, impliedly precluding a remedy for injunctive relief. In addition, as also already explained, the FISC-authorized collection under § 1845(a) lapsed in 2011.

response to a production order, are *not* made actionable under section 2712.[17] Congress further stipulated that an action under § 2712 shall be the exclusive remedy against the United States for claims falling within its purview. *Id*. § 2712(d). Section 2712 thus deals with claims for misuses of information obtained under FISA in great detail, including the intended remedy, and Plaintiffs cannot rely on section 702 to bring a claim for violation of FISA's terms that Congress did not provide for under 18 U.S.C. § 2712. *Pottawatomi Indians*, 132 S. Ct. at 2205. The same conclusion was reached by the district court in *Jewel*, *supra,* which held that § 2712, "by allowing suits against the United States only for damages based on three provisions of [FISA], impliedly bans suits against the United States that seek injunctive relief under any provision of FISA." 2013 WL 3829405, at *12.

III. PLAINTIFFS' CLAIM THAT THE ALLEGED NSA INTELLIGENCE-GATHERING PROGRAMS EXCEED THE GOVERNMENT'S STATUTORY AUTHORITY IS ALSO UNLIKELY TO SUCCEED ON THE MERITS

Even if judicial review of Plaintiffs' statutory claim were not precluded, the claim lacks merit. Plaintiffs assert that "Defendants' surveillance program" is unauthorized under Section 215 because (i) the records obtained by the NSA are not "relevant" to authorized national security investigations, and (ii) the FISC may not prospectively direct the production of business records that do not yet exist. *Klayman I* Br. at 17-19; *Klayman II* Br. at 19-21. The Government Defendants address Plaintiffs' arguments first as they apply to the telephony metadata program, and then as they apply (or, rather, do not apply) to the NSA's collection of bulk Internet metadata and of communications targeted under Section 702.

[17] The enactment of section 223 of the USA PATRIOT Act in 2001 preceded enactment of 50 U.S.C. § 1861(h) in 2006. 1 Kris & Wilson § 19:11 at 718. Congress has not since amended § 2712 to include violations of § 1861(h) as a basis for suit. In fact, when Congress amended Section 215 to add subsection (h), it also added the review provision at subsection (f), but made review available only to persons to whom Section 215 orders are directed.

A. The Telephony Metadata Program Is Authorized Under Section 215

Section 215 authorizes the FISC to order "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), (b)(2)(A). Since May 2006, fifteen separate judges of the FISC have concluded on thirty-five occasions that the Government 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; Aug. 29 FISC Op. at 28; Oct. 11 FISC Mem., Primary Order, at 2. Plaintiffs now ask this Court to second-guess the FISC's repeated conclusions and declare instead that the call-detail records the FISC order produced to the NSA are not, in fact, relevant to authorized counter-terrorism investigations. The Court should reject this invitation.

1. Bulk telephony metadata are "relevant" within the meaning of Section 215.

The concept of "relevance" has developed an accepted legal meaning in the context of official investigations and civil proceedings, for which purposes documents are considered "relevant" not only where they directly bear on a matter, but also where they reasonably could lead to other information that may bear on the matter. In civil discovery, for example, the phrase "relevant to the subject matter involved in the pending action" broadly encompasses "any matter that bears on, *or that reasonably could lead to other matters that could bear on*, any issue that is or may be in the case." *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978) (emphasis added). An even broader relevance standard applies to grand jury subpoenas, which will be enforced 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."

United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991) (emphasis added). Likewise, the statutory authority conferred on administrative agencies to subpoena evidence that is "relevant to [a] charge under investigation" affords them "access to virtually any material that might cast light on the allegations" at issue in an investigation, *EEOC v. Shell Oil Co.*, 466 U.S. 54, 68-69 (1984) (internal quotations omitted).

In light of that basic understanding of relevance, courts in each of these contexts have categorically authorized the production of entire repositories of records, even when any particular record is unlikely to bear directly on the matter being investigated, where searching a large volume of information is the only feasible means of locating much smaller amounts of critical information within the data that directly bears on the matter under investigation.[18] Analogously, courts also issue search warrants permitting Government agents to copy entire computer hard drives and then later review their contents for the specific evidence described in the warrant. *See* Fed. R. Crim. P. 41(e)(2)(B).[19] These practices demonstrate the broad understanding of relevance developed in the context of investigatory information-gathering.

---

[18] *See, e.g., In re Subpoena Duces Tecum*, 228 F.3d 341, 350-51 (4th Cir. 2000) (subpoena for 15,000 patient files); *In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987) (upholding grand jury subpoenas for records of wire money transfers "involving hundreds of innocent people"); *FTC. v. Invention Submission Corp.*, 965 F.2d 1086 (D.C. Cir. 1992); *Carrillo Huettel, LLP v. SEC*, 2011 WL 601369, at *2 (S.D. Cal. Feb. 11, 2011) (trust account information for all of law firm's clients held relevant to SEC investigation); *Goshawk Dedicated Ltd. v. American Viatical Servs., LLC*, 2007 WL 3492762, at *1 (N.D. Ga. Nov. 5, 2007) (compelling production of business's entire underwriting database); *In re Adelphia Commc'ns Corp.*, 338 B.R. 546, 549 and 553 (Bankr. S.D.N.Y. 2005) (permitting inspection of "approximately 20,000 large bankers boxes of business records"); *Medtronic Sofamor Danek, Inc. v. Michelson*, 229 F.R.D. 550, 552 (W.D. Tenn. 2003) (compelling discovery of "approximately 996 network backup tapes . . . plus an estimated 300 gigabytes of other electronic data").

[19] *See, e.g., United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006) (recognizing that "blanket seizure" of the defendant's entire computer system, followed by subsequent review, may be permissible); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999).

Both the text and legislative history confirm that Congress was acutely aware of and incorporated this accepted legal meaning of relevance when it enacted Section 215's relevance requirement, *see* USA PATRIOT Act Improvement Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192 (2006). It was well understood at the time that relevance was the equivalent of the "well established standard" applied to grand jury subpoenas, administrative subpoenas, and civil discovery requests. *See* 152 Cong. Rec. S1598, 1606 (Mar. 2, 2006) (statement of Sen. Kyl).[20] And Congress in fact described the items subject to production under Section 215 as things obtainable by "a subpoena duces tecum issued by a court . . . in aid of a grand jury investigation" or "any other order issued by a court . . . directing the production of records or tangible things." 50 U.S.C. § 1861(c)(2)(D).[21]

Of course, the case law in the contexts of civil discovery, grand jury subpoenas, and administrative investigations does not involve data acquisition on the scale of the telephony metadata collection authorized by the FISC, because the information gathered in those contexts is sought in aid of focused judicial and administrative proceedings involving identifiable individuals and events. But in this context relevance must be evaluated in light of the special nature, purpose, and scope of national security investigations. *See Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 209 (1946). Counter-terrorism investigations serve uniquely important purposes beyond the ambit of routine criminal or administrative inquiries, which ordinarily focus

[20] *See also* 152 Cong. Rec. S1379, 1395 (Feb. 16, 2006) (statement of Sen. Kyl) ("We all know the term 'relevance.' It is a term that every court uses . . . The relevance standard is exactly the standard employed for the issuance of discovery orders in civil litigation, grand jury subpoenas in a criminal investigation, and for each and every one of the 335 different administrative subpoenas currently authorized by the United States Code."); 151 Cong. Rec. S13636, 13642 (Dec. 15, 2005) (statement of Sen. Hatch); H.R. Rep. No. 109-174, pt. 1 at 131 (statement of Rep. Lungren).

[21] *See also NLRB v Amax Coal Co.*, 453 U.S. 322, 329 (1981) ("Where Congress uses terms that have accumulated settled meaning under either equity or the common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of these terms.").

retrospectively on specific crimes or violations that have already occurred and the persons known or suspected to have committed them. The key purpose of terrorism investigations is to prevent terrorist attacks before they occur. Hence, national security investigations often have remarkable breadth, spanning long periods of time and multiple geographic regions to identify terrorist groups, their members, intended targets, and means of attack, many of which are often unknown to the intelligence community at the outset. *See CIA v. Sims,* 471 U.S. 159, 171 (1985) ("foreign intelligence [gathering] consists of securing all possible data pertaining to . . . the national defense and security of the United States"); *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 322-23 (1972). Relevance in this context, therefore, must take into account the far-reaching information-gathering required to shed light on suspected terrorist organizations, their size and composition, recruitment, geographic reach, relation to foreign powers, financial resources, past acts, goals, and capacity for carrying out their plans.

When Congress codified the relevance standard under Section 215, the critical differences between the breadth and attributes of counter-terrorism investigations and routine criminal investigations were well understood. *See* H.R. Rep. No. 109-174(1) at 129 (statement of Rep. Lungren) ("[t]his is in the nature of trying to stop terrorists before they act, not in the nature of a regular criminal investigation . . . and it strikes . . . precisely at when a 215 order is most useful"); *see also* 152 Cong. Rec. S1325, 1330 (Feb. 15, 2006) (statement of Sen. Feingold). The purpose underlying the USA PATRIOT Act, and Section 215 in particular, was to provide the intelligence community the enhanced investigatory tools needed to bring terrorist activities to light before they culminate in a loss of life and property. *See* H.R. Rep. No. 109-174, pt. 2 at 4 ("[M]any of the core enhanced authorities of the [Patriot Act] are fundamentally intelligence authorities intended to gather information to counter threats to national security from terrorists."); S. Rep. No. 109-85 at 40 (noting "critical" nature and "broad reach" of authority

conferred by Section 215). Consistent with this core legislative objective, Section 215 should be understood to authorize the collection of records that can help to identify previously unknown operatives and activities, and thus detect and prevent terrorist attacks before they are launched.

Bulk telephony metadata are therefore relevant (at the least) to FBI counter-terrorism investigations because, as experience has shown, the collection and aggregation of these data permit the effective use of NSA analytical tools to detect contacts between foreign terrorists and their unknown associates located in the United States who may be planning attacks on the U.S. soil. Holley Decl. ¶¶ 8-9, 18-26; Shea Decl. ¶¶ 44, 46-48; *see* Aug. 29 FISC Op. at 20. 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 the creation of an historical repository of information that bulk collection and aggregation of the data allow, it may not be feasible for NSA to identify chains of communications among known and unknown terrorist operatives that cross different time periods and providers' networks. Holley Decl. ¶¶ 9, 27-29; Shea Decl. ¶ 60; *see* Aug. 29 FISC Op. at 21-22. Thus, there are reasonable grounds, at the least, for concluding that "the whole of the metadata produced" is "relevant" to authorized national security investigations. Aug. 29 FISC Op. at 22.[22]

[22] Notably in this regard, Section 215 permits the collection of information relevant "to an authorized investigation," 50 U.S.C. § 1861(b)(2)(A), not simply information relevant to the "subject matter" involved a matter, as in civil discovery, Fed. R. Civ. P. 26(b)(1). Business records can therefore be "relevant" to an investigation not merely if they relate to its subject matter, but also if there is reason to believe they are necessary or useful to the application of investigative techniques that will advance its purposes. As discussed above, NSA analysis enables discovery of otherwise hidden connections between individuals suspected of engaging in terrorist activity and unknown co-conspirators with whom they maintain contact in the United States. The metadata records are therefore relevant to FBI investigations whose object is to thwart the plots in which these individuals are engaged before they come to bitter fruition.

2. Congress has legislatively ratified the construction of Section 215 as allowing for the bulk collection of telephony metadata records

That conclusion is reinforced, as the FISC recently recognized, by Congress's extension of Section 215's authorization without substantive 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. On both occasions the Executive Branch worked to ensure that *all* Members of Congress had access to information about this program and the legal authority for it. In December 2009, a classified briefing paper, explaining that the Government and the FISC had interpreted Section 215 to authorize the bulk collection of telephony metadata, was provided to the House and Senate Intelligence Committees and made available for review, as well, by all Members of Congress, "to inform the legislative debate about reauthorization of Section 215."[23] Additionally, the classified use of this authority has been briefed numerous times over the years to the Senate and House Intelligence and Judiciary Committees, as several Members of Congress have acknowledged.[24]

---

[23] *See* Letter from Ronald Weich to Rep. Silvestre Reyes (Dec. 14, 2009) (Exh. K, hereto); Report on the [NSA's] Bulk collection Programs for USA PATRIOT Act Reauthorization (Exh. L, hereto). Both Intelligence Committees made this document available to all Members of Congress prior to the February 2010 reauthorization of Section 215. *See* Letter from Sens. Feinstein and Bond to Colleagues (Feb. 23, 2010) (Exh. M, hereto); Letter from Rep. Reyes to Colleagues (Feb. 24, 2010) (Exh. N, hereto); *see also* 156 Cong. Rec. H838 (daily ed. Feb. 25, 2010) (statement of Rep. Hastings); 156 Cong. Rec. S2109 (daily ed. Mar. 25, 2010) (statement of Sen. Wyden).

An updated version of the briefing paper was provided to the Senate and House Intelligence Committees again in February 2011 in connection with the reauthorization that occurred later that year. *See* Letter from Ronald Weich to Sens. Diane Feinstein and Saxby Chambliss (Feb. 2, 2011) (Exh. O, hereto); Letter from Ronald Weich to Reps. Mike Rogers and C.A. Dutch Ruppersberger (Feb. 2, 2011) (Exh. P, hereto). The Senate Intelligence Committee made this updated paper available to all Senators later that month. *See* Letter from Sens. Feinstein and Chambliss to Colleagues (Feb. 8, 2011) (Exh. Q, hereto).

[24] *See* Press Release of Sen. Select Comm. on Intelligence (June 6, 2013) (Exh. Q, hereto)); *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our*

After receiving these "extensive and detailed" briefing papers "regarding the nature and scope" of the program, Congress twice extended Section 215's authorization, in 2010 and 2011. Aug. 29 FISC Op. at 25 & n.23.[25] "'Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change.'" *Forest Grove Sch. Dist. v. T.A.*, 557 U.S. 230, 239-40 (2009) (quoting *Lorillard v. Pons*, 434 U.S. 575, 580 (1978)). That presumption is ironclad in this instance, where Congress had actual and repeated notice of the Executive Branch's administrative construction of Section 215 over a period of years.[26] Imposing a limiting construction now on Section 215 that would prohibit bulk collection of telephony metadata would be contrary to the express understanding of the statute that Congress ratified on two separate occasions.

3. Plaintiffs present no persuasive reasons for concluding that bulk telephony metadata are not "relevant" to authorized counter-terrorism investigations within the meaning of Section 215

Plaintiffs nevertheless maintain that the NSA's bulk collection of telephony metadata exceeds the Government's authority under Section 215 because it disregards the relevance requirement. But since May 2006, fifteen separate judges of the FISC have concluded otherwise,

---

Adversaries: Hearing Before the House Perm. Select Comm. on Intelligence 2, 35, 58, 113th Cong., 1st Sess. (2013) (statements of Reps. Rogers, Langevin, and Pompeo) (Exh. R, hereto).

[25] USA PATRIOT Act – Extension of Sunsets, Pub. L. No. 111-141, § 1(a), 124 Stat. 37; PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, § 2(a), 125 Stat. 216.

[26] *See EEOC v. Shell Oil Co.*, 466 U.S. 54, 69 & n.21 (1984), *and Haig v. Agee*, 453 U.S. 280, 297-98 & n.37 (1981) (both finding "clear[ ]" and "undoubted" Congressional awareness of the pertinent judicial and executive interpretations, based on references in committee reports).

Moreover, in both 2009 and 2011, when the Senate Judiciary Committee was considering possible amendments to Section 215, it made clear that it had no intention of affecting the telephony metadata collection program. The Committee reports accompanying the USA PATRIOT Act Sunset Extension Acts of 2009 and 2011 explained that proposed changes to Section 215 were "not intended to affect or restrict any activities approved by the FISA court under existing statutory authorities." S. Rep. No. 111-92, at 7 (2009); S. Rep. No. 112-13, at 10 (2011). Ultimately, Section 215 was extended to June 1, 2015 without change. *See* Patriot Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011).

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; Oct. 11 FISC Mem. at 3. As the FISC concluded recently:

> [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; *see also* Oct. 11 FISC Mem. at 3.

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 should substitute its judgment for the decisions that the FISC reached thirty-five times.

That approach cannot be reconciled with the legislative plan. When courts are called on to enforce grand jury or administrative subpoenas—instruments that informed Congress's understanding of Section 215, *see supra* at 34-35, — the Government's determination that records are "relevant" to its investigation is subject only to the most deferential review.[27] In the analogous context of electronic surveillance, FISC orders receive only "minimal scrutiny by

[27] *See R. Enters.*, 498 U.S. at 301 (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"); *FTC v. Invention Submission Group*, 965 F.2d 1086, 1089 (D.C. Cir. 1992) (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") .

[reviewing] courts." *See, e.g., United States v. Abu-Jihaad*, 630 F.3d 102, 130 (2d Cir. 2010); *United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008).

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 Court would have to conclude that the fifteen FISC judges who repeatedly issued those orders lacked any reasonable basis for doing so. That proposition is self-defeating. The fact that fifteen 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 to the contrary.

At bottom, Plaintiffs argue that bulk telephony metadata cannot be considered relevant under Section 215 because the vast majority of the data collected do not pertain to persons who "are subjects of an authorized investigation," or who are reasonably suspected, based on "specific and articulable facts," of terrorist activity. *Klayman I* Br. at 17-18. This argument fails, however, because 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; *see* Aug. 29 FISC Op. at 13. Again 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.[28] Limiting the reach of Section 215 to specific records bearing directly on known terrorist threats and operatives would inhibit the use of this authority for its intended purposes—detecting unknown terrorist threats—and frustrate, not vindicate, the will of Congress.

Moreover, Plaintiffs' underlying complaint, that the "vast majority" of call-detail records collected by the NSA are not related to specific counter-terrorism investigations, *Klayman I* Br. at 18, comes as no 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 supra* at 34-37; Aug. 29 FISC Op. at 20-23; Shea Decl., ¶ 5, 23-24. 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 NSA cannot know in advance of making authorized queries (under the "reasonable articulable suspicion" standard) 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 evidence that the Government (or the FISC) has exceeded its authority, but an outgrowth of the leeway that Congress extended to the Government to obtain foreign intelligence information under Section 215 "to meet its national security responsibilities." *Id*. at 23. As the FISC has recognized, Congress anticipated this prospect, and

[28] *See* S. 2369, 109th Cong. § 3, *reprinted at* 152 Cong. Rec. S1791 (Mar. 6, 2006); 151 Cong. Rec. S14275-01 (Dec. 21, 2005) (statement of Sen. Dodd) ("Unfortunately, the conference report . . . maintains the minimal standard of relevance without a requirement of fact connecting the records sought, or the individual, [to] suspected . . . terrorist activity"). *See also* 152 Cong. Rec. S1598-03 (2006) (statement of Sen. Levin); 152 Cong. Rec. H581-02 (Mar. 7, 2006) (statement of Rep. Nadler).

so 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; Shea Decl. ¶¶ 29-35.

In the final analysis, Plaintiffs succeed only in demonstrating 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 granted to it. 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.

4. Nothing in Section 215 prohibits the FISC from prospectively directing the production of business records as they are created

Plaintiffs' next contention, that Section 215 does not authorize the collection of business records "not yet in existence," *Klayman I* Br. at 17, is erroneous as a matter of law. Section 215 authorizes the FISC to direct the production of "*any* tangible things," "documents," or "records." 50 U.S.C. § 1861(a)(1)(emphasis added). Nothing in the text of the statute suggests that FISC orders may apply only to records created before the FISC renders its order. Nor do the FISC's orders require the creation or preservation of documents that would otherwise not exist, or compel telecommunications service providers to retain information they would otherwise discard. For example, telephony metadata such as the records at issue here are routinely created and maintained by providers for at least 18 months, pursuant to Federal Communications Commission regulations. *See* 47 C.F.R. § 42.6.

Prospective production of business records has been deemed appropriate in analogous contexts. For example, under the SCA, the Government may obtain a court order requiring a

provider of cell-phone service to produce non-content "record[s] or other information pertaining to a subscriber . . . or customer" on a specific showing of "reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(c)(1), (d). Courts have held that the Government may seek prospective disclosure of records under the SCA because "the prospective . . . information sought by the Government . . . becomes a 'historical record' as soon as it is recorded by the provider," and the statute "in no way limits the ongoing disclosure of records to the Government as soon as they are created." *In re Application of the United States,* 632 F. Supp. 2d 202, 207 n.8 (E.D.N.Y. 2008).[29] Like the SCA, there is nothing in the text or legislative history of Section 215 indicating that Congress meant to prohibit contemporaneous production to the Government of business records that are generated on a daily basis. This approach does not provide the Government with indefinite access to bulk telephony metadata, as Plaintiffs suggest, *see Klayman I* Br. at 19, as the Government must obtain a new order for production of these metadata every 90 days. *See supra* at 9.[30]

Plaintiffs have demonstrated no likelihood of success on their claim that the NSA's collection of bulk telephony metadata exceeds the Government's authority under Section 215.

---

[29] *See also United States v. Booker*, 2013 WL 2903562, at *6-7 (N.D. Ga. June 13, 2013); *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*, 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006); *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).

[30] 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.

B. Plaintiffs Have No Likelihood of Success on Their Statutory Challenge to the Government's Targeted Collection Directed Against non-U.S. Persons Located Outside the United States

To the extent Plaintiffs mean to argue that the Government has also engaged in "bulk acquisition" of the *content* of Americans' electronic communications, in excess of the authority conferred by Section 215, *see Klayman II* Br. at 13-15, 19-21, their argument is misguided as a matter of fact and law.

As discussed above, Section 702 of FISA authorizes the Government to conduct surveillance that targets non-U.S. persons located outside the United States to acquire foreign intelligence information, 50 U.S.C. § 1881a(a), (b), subject to FISC approval of the Government's procedures to ensure lawful targeting of its surveillance and minimization of the acquisition, retention, and dissemination of non-public information about non-consenting U.S. persons, *id*. § 1881a(i)(2)-(3). The Government has acknowledged its use of this authority to target non-U.S. persons located abroad. *See supra* at 13-15. Plaintiffs have adduced no evidence, however, that the Government has ever collected the *contents* of electronic communications in bulk—whether of American citizens or otherwise—or that it has ever collected the contents of such communications, in bulk or otherwise, under authority of Section 215.

C. Plaintiffs Have No Likelihood of Success on Their Statutory Challenge to the Government's Prior Collection of Bulk Internet Metadata

Plaintiffs similarly maintain that the collection of bulk Internet metadata exceeds the Government's authority under Section 215, on the ground that bulk collection of Internet metadata does not comport with Section 215's relevance requirement. *Klayman II* Br. at 19-21. To the extent Plaintiffs are referring to the FISC-authorized bulk collection of Internet metadata recently declassified by the DNI, the DNI has explained that the program was discontinued in

2011, and thus there is no current collection to enjoin that warrants consideration of whether that activity exceeded statutory authority. Second, as also explained above, that program of bulk Internet metadata collection was authorized by the FISC under authority of the pen/trap statute, 50 U.S.C. § 1842 (not Section 215).[31] Accordingly, Plaintiffs' allegations concerning the bulk collection of Internet metadata cannot support an award of preliminary injunctive relief.

In sum, Plaintiffs have demonstrated no likelihood of success on the merits of their claims against the Government Defendants.

IV. PLAINTIFFS CANNOT SUCCEED ON THE MERITS OF THEIR FOURTH AMENDMENT CLAIM BECAUSE THE CHALLENGED SURVEILLANCE DOES NOT VIOLATE PLAINTIFFS' FOURTH AMENDMENT RIGHTS

A. Plaintiffs Have No Fourth Amendment Privacy Interest in Telecommunications Metadata

The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." As the Supreme Court remarked just last year, "for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates." *United States v. Jones*, 132 S. Ct. 945, 949-50 (2012). In addition to the core concern over searches and seizures within these enumerated areas, it is now understood that a Fourth Amendment "search" takes place when the government's investigative activities "violate a person's 'reasonable expectation of privacy.'" *Id.* (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967)).

The Government's collection of telephony metadata pursuant to orders of the FISC does not involve a "search" of individual subscribers or their property. The orders are directed to telecommunications service providers, not to subscribers, and direct the production of what are

[31] Moreover, the FISC has previously found that bulk collection of information comports with the relevance requirement of the pen/trap statute. *See* Aug. 29 FISC Op. at 19-20.

indisputably the providers' own business records. Nor do telephone subscribers have a reasonable expectation of privacy in telephony metadata. In *Smith v. Maryland*, 442 U.S. 735, 741-46 (1979), the Supreme Court held that the government's recordation of numbers dialed from an individual's home telephone, through a pen register installed at the telephone company's central offices, did not constitute a search of that individual under the Fourth Amendment, because persons making telephone calls, even from their own homes, lack a reasonable expectation of privacy in the numbers they call. In contrast to the contents of telephone calls, the Court held that there is no reasonable expectation of privacy in the telephone numbers dialed, because telephone users "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes," such as billing and fraud detection. *Id.* at 743.

Furthermore, the Court reasoned, even if a subscriber harbored a subjective expectation that the phone numbers he dialed would remain private, such an expectation of privacy would not be reasonable, because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44. The Court explained that someone who uses a phone has "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," and therefore has "assumed the risk that the company would reveal to police the numbers he dialed." *Id.* at 744. 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 records.[32]

[32] *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

Smith is fatal to Plaintiffs' claim that the collection of their telephony metadata violates the Fourth Amendment. *See* 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."). So far as metadata include such information as the times and duration of calls and the numbers of the parties with whom they spoke, that is information that telephone subscribers voluntarily turned over to their providers. The remaining data, such as trunk identifiers, is information generated by the phone companies themselves. *See* Primary Order at 3 n.1. Call-detail records memorializing this information belong to the phone companies, as the parties providing the equipment and services required to make those calls possible. *See United States v. Miller*, 425 U.S. 435, 440-41 (1976) (rejecting a bank depositor's Fourth Amendment challenge to a subpoena of bank records because, inasmuch as the bank was a party to the transactions, the records belonged to the bank). Thus, under *Smith*, there can be no reasonable expectation of privacy in this information, even if—as has not been alleged here—there were an understanding that the third party (*i.e.*, the telephone company) would treat the information as confidential. *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984); *Miller*, 425 U.S. at 443.

Importantly, the call-detail records reveal only phone numbers and other numeric data, not any information identifying the caller or the person called. *See* Shea Decl. ¶¶ 15, 21; Holley Decl. ¶¶ 7, 11. Thus, these data do not in fact reveal any information about the subscriber's professions, political activities, or other activities in which they may have a privacy interest. *See Klayman I* Br. at 20; *Klayman II* Br. at 21-22. The mere fact that the numbers dialed from a phone could, in some hypothetical sense, reveal the identities of the persons and the places

---

(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).

called, was raised by the dissenters in *Smith*, 442 U.S. at 748 (Stewart, J., dissenting), but the Court nonetheless ruled that there is no reasonable expectation of privacy in telephone numbers dialed. *Id*. at 741-42; *see also U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 454 (D.C. Cir. 2000) ("telephone numbers are not protected by the Fourth Amendment") (citing *Smith*).

Remarkably, Plaintiffs fail to even cite, let alone attempt to distinguish, *Smith*. Instead, they rely on Justice Sotomayor's concurring opinion in *United States v. Jones*, 132 S. Ct. 945 (2012), for the proposition that "Plaintiffs' expectation that their communication records will not be subject to long-term recording, aggregation, and surveillance by the government[] is objectively reasonable, particularly as the intrusive surveillance at issue allows the government to gather intricate details of each individual and their associations with one another, including their clients, supporters, and membership." *Klayman I* Br. at 20, *Klayman II* Br. at 22. Justice Sotomayor expressed concern that the GPS monitoring at issue in *Jones*, which the Court held constituted a search under a trespass theory completely inapplicable here, "'generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.'" *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, however, the bulk telephony metadata program provides the NSA with information about calls between unidentified phone numbers, when the calls occurred, and how long they lasted. Thus, unlike in *Jones*, the NSA does not know the identity of anyone making or receiving the calls (apart,

perhaps, from the suspected terrorist actors associated with the "seed" identifiers), and under the terms of the FISC's orders, cannot use the metadata to detail individuals' associations.[33]

Nor does the scope of the telephony metadata collection under the FISC's orders alter the Fourth Amendment analysis. Fourth Amendment rights "are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched." *Steagald v. United States*, 451 U.S. 204, 219 (1981); *accord, e.g.*, *Minnesota v. Carter*, 525 U.S. 83, 88 (1998); *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978). No Fourth Amendment-protected interest of Plaintiffs is implicated, therefore, by virtue of the fact that the metadata of many other individuals' calls are collected as well as their own. *See In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987) (rejecting argument that a subpoena was unreasonable under the Fourth Amendment because it "may make available to the grand jury [money transfer] records involving hundreds of innocent people"); *United States v. Rigmaiden*, 2013 WL 1932800, at *13 (D. Ariz. May 8, 2013) (Government did not violate defendant's Fourth Amendment rights by acquiring a high volume (1.8 million) of IP addresses).

Courts have also specifically applied the reasoning of *Smith* to find no reasonable expectation of privacy in Internet metadata, finding the use of a pen register to obtain data such as the to/from addresses of email messages to be "constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*." *United States v. Forrester*, 512 F.3d 500,

[33] For this reason, even in the absence of *Smith*, the mere collection of Plaintiffs' telephony metadata under the Section 215 program, without review of the data pursuant to a query made under "reasonable articulable suspicion" standard, would not rise to the level of a search under the Fourth Amendment, because the Government's acquisition of an item without examining its contents "does not compromise the interest in preserving the privacy of its contents." *Horton v. California*, 496 U.S. 128, 142 n.11 (1990). *See also United States v. Van Leeuwen*, 397 U.S. 249, 252-53 (1970) (defendant's interest in the privacy of his detained first-class mail "was not disturbed or invaded" until the Government searched the packages).

510 (9th Cir. 2008).[34] Thus, Plaintiffs have no Fourth Amendment privacy interest in the collection of internet metadata either, and the acknowledged internet metadata collection program has ceased. It is therefore not necessary to address its reasonableness (which in any event tracks the reasonableness of the telephony metadata collection), even if its collection amounted to a search (which it did not under *Smith* and its progeny).

B. The Government's Acquisition of Telephony Metadata Is Reasonable

Even if collecting telephony metadata involved a Fourth Amendment "search" (it does not), the Fourth Amendment bars only "unreasonable" searches and seizures, whereas the collection of metadata at issue here is reasonable under the standard the Supreme Court applies to assess suspicionless searches that serve special government needs. As the Supreme Court has explained, "where a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context." *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665-66 (1989). More specifically, the scope of the legitimate expectation of privacy and the character of the intrusion are balanced against the nature of the government interests to be furthered, as well as the immediacy of the government's concerns regarding those interests and the efficacy of the policy at issue in addressing those concerns. *See Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 658, 660, 662-63 (1995).

---

[34] *See also Guest v. Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001); *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 131-38 (E.D. Va. 2011) (Internet protocol ("IP") address information); *United States v. Qing Li*, No. 07 CR 2915 JM, 2008 WL 789899, at *4-5 (S.D. Cal. Mar. 20, 2008) (IP log-in histories and addressing information). As the Court explained in *Forrester*, email and internet users also rely on third-party companies and equipment to engage in their communications; and email to/from addresses and IP addresses are addressing information and do not necessarily reveal any more about the contents of communications than do phone numbers. 512 F.3d at 510-11.

The NSA's collection of telephony metadata clearly serves special governmental needs above and beyond normal law enforcement. The undisputed programmatic purpose of the collection of this metadata is identifying unknown terrorist operatives and preventing terrorist attacks—forward-looking goals that fundamentally differ from most ordinary criminal law enforcement, which typically focuses on solving crimes that have already occurred, not protecting public safety and national security. The Supreme Court has distinguished between domestic-security surveillance and surveillance in connection with ordinary crime:

> The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime . . . . Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.

United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 322-23 (1972). *See also Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls*, 536 U.S. 822, 828 (2002) (the probable cause standard "is peculiarly related to criminal investigations and may be unsuited to determining the reasonableness of administrative searches where the Government seeks to *prevent* the development of hazardous conditions.") (internal quotations omitted); *Abu-Jihaad*, 630 F.3d at 122 (extending the distinction noted in *Keith* to foreign intelligence surveillance); *In re Sealed Case*, 310 F.3d 717, 746 (FISC-R 2002) ("FISA's general programmatic purpose, to protect the nation against terrorists and espionage threats directed by foreign powers, has from its outset been distinguishable from 'ordinary crime control.'").

If, contrary to *Smith*, Plaintiffs could be said to have any Fourth Amendment privacy interest that is implicated by collection of non-content telephony metadata, that interest would be minimal. Moreover, the intrusion on that interest would be mitigated still further by the

statutorily mandated restrictions on access to and dissemination of the metadata that are written into the FISC's orders. *See* Primary Order, at 4-14. *See also Maryland v. King*, 133 S. Ct. 1958, 1979 (2013) (safeguards limiting DNA analysis to identification information alone reduced any intrusion into privacy); *Board of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls*, 536 U.S. 822, 833 (2002) (restrictions on access to drug-testing results lessened intrusion on privacy); *Vernonia Sch. Dist.*, 515 U.S. at 658 (intrusion of urine-testing on privacy was reduced by fact that student athletes were tested only for illegal drugs and not for medical condition).

On the other side of the balance, the collection and analysis of telephony metadata promote overriding public interests. The Government's interest in identifying and tracking terrorist operatives for the purpose of preventing terrorist attacks is a national security concern of overwhelming importance. *See Haig v. Agee*, 453 U.S. 280, 307 (1981) ("no governmental interest is more compelling than the security of the Nation.") (internal quotation marks omitted); *In re Directives*, 551 F.3d 1004, 1012 (FISC-R 2008) ("the relevant governmental interest—the interest in national security—is of the highest order of magnitude."). Requiring individualized suspicion here would indeed be impracticable. The Government's interests in identifying unknown terrorist operatives and preventing terrorist attacks cannot be as effectively achieved by requiring individualized suspicion to collect metadata, because such a requirement would not permit the type of historical analysis and contact chaining that the broader collection enables and to quickly identify contacts. *See* Aug. 29 FISC Op. at 20-22; Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization, at 5. Thus, given that the program might be rendered entirely infeasible, it would certainly be "impracticable" to require individualized suspicion in this context. *See Von Raab*, 489 U.S. at 665-66.

Thus, even if Plaintiffs had a reasonable expectation of privacy in telephony metadata, which they do not, the NSA's acquisition of these data is reasonable and does not violate Plaintiffs' Fourth Amendment rights.

C. The NSA's PRISM Collection Does Not Violate Plaintiffs' Fourth Amendment Rights

To the extent the Klayman II motion for preliminary injunction claims that the NSA's PRISM collection violates Plaintiffs' Fourth Amendment rights, Plaintiffs are unlikely to succeed on the merits of this claim as well. The Government has acknowledged that the NSA targets non-U.S. persons located overseas under its PRISM collection, pursuant to Section 702 of the FISA. *See* Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *9 n.24; IC's Collection Programs Under Title VII of the FISA, at 3. As discussed above, Plaintiffs have not alleged any facts that would suggest that their communications have been either targeted or incidentally collected under the PRISM collection, which in and of itself prevents them from succeeding on such a claim. But even if they could get past this hurdle, their Fourth Amendment claim would still fail because (i) the PRISM collection may target only non-U.S. persons located outside the United States, who lack Fourth Amendment rights altogether; (ii) any privacy interests in communications incidentally intercepted in a Section 702 acquisition are protected through minimization procedures required by Section 702 and approved by the FISC; (iii) foreign intelligence-gathering comes within the special governmental needs exception to the warrant requirement; and (iv) the PRISM collection is reasonable.

Section 702 acquisitions may target only non-U.S. persons located outside the United States—who lack Fourth Amendment rights to begin with. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990) (holding that only persons who "have come within the territory of the United States and developed substantial connections" to the country have Fourth

Amendment rights). Because the Fourth Amendment does not protect such persons in the first instance, it cannot prevent the Government from subjecting them to surveillance without a warrant. To the extent Plaintiffs' claim is that their communications were collected incidentally under the PRISM collection, the "incidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment." *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) (citing, *inter alia*, *United States v. Kahn*, 415 U.S. 143, 157 (1974) (holding that interception of wife's communications incident to lawful wiretap targeting husband's communications did not violate the Fourth Amendment)). If it were otherwise, virtually all surveillance of foreign targets abroad would require a warrant, because there is almost always the possibility that a foreign target may communicate with a U.S. person.

Had any of Plaintiffs' communications been incidentally intercepted under PRISM, their privacy interests in those communications would be protected by the minimization procedures approved by the FISC under Section 702. By definition, minimization procedures under FISA must be reasonably designed to minimize the acquisition and retention, and to prohibit the dissemination, of private information concerning U.S. persons, to the extent consistent with the Government's need to obtain, produce, and disseminate foreign intelligence information. 50 U.S.C. § 1801(h). In other words, such procedures by design aim to ensure that any intrusion on the privacy of U.S. persons is reasonably balanced against governmental intelligence needs. Such minimization procedures have been held constitutionally sufficient to protect third-parties in the domestic law enforcement context. *See, e.g.*, *United States v. Figueroa*, 757 F.2d 466, 471 (2d Cir. 1985) ("Innocent parties are protected from unreasonable surveillance by the requirement contained in [Title III] that surveillance 'shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception.'") (citing *Scott v. United States*, 436 U.S. 128, 130-31 (1978)). This conclusion applies fully—if not more

forcefully—in the foreign intelligence context. *See, e.g.*, *In re Sealed Case*, 310 F.3d at 740-41 (FISA's requirement of minimization procedures supports statute's reasonableness).

Moreover, foreign intelligence-gathering serves a purpose beyond the normal need for law enforcement and therefore comes within the special governmental needs exception to the warrant requirement. As the FISC Court of Review has held, the Government's "programmatic purpose" in obtaining foreign intelligence information is "to protect the nation against terrorist and espionage threats directed by foreign powers—'a special need' that fundamentally differs from 'ordinary crime control.'" *In re Sealed Case*, 310 F.3d at 717. And, more specifically, the FISC "has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within the 'foreign intelligence exception' to the warrant requirement of the Fourth Amendment." Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *24.

Monitoring foreign targets located overseas under Section 702 is critical to protecting against foreign threats to national security and thus serves governmental interests of the highest order. Balanced against these important interests are the privacy interests of U.S. persons whose communications may be collected incidentally, but, as discussed above, any such interests are adequately protected by Section 702's minimization procedures. The safeguards built into the statute provide reasonable assurance that the surveillance it authorizes will target only foreign persons outside the United States and will be conducted in a way that minimally affects the privacy of U.S. persons. The Fourth Amendment requires no more.

V. PLAINTIFFS CANNOT DEMONSTRATE THAT THEY ARE LIKELY TO SUCCEED ON THEIR FIRST AMENDMENT CLAIM

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

Plaintiffs' First Amendment claim, that the metadata and content collections violate their freedom of speech and association, *Klayman I* Br. at 22-26; *Klayman* II Br. at 24-28, perishes in

the wake of their failed Fourth Amendment claim. Recognizing the need to accommodate the Government's interests where prevention of crime, or, even more imperatively, potential threats to national security are concerned, *see ACLU Found. v. Barr*, 952 F.2d 457, 471 (D.C. Cir. 1991), courts distinguish for purposes of First Amendment analysis between government investigations that may have the incidental effect of deterring First Amendment activity, and concrete government action of a regulatory, proscriptive, or compulsory nature that is directed against individuals based on their expressive or associational activities. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *Laird*, 408 U.S. at 11; *Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1051-53 (D.C. Cir. 1978). Accordingly, the law is clear that good faith governmental investigations conducted in observance of Fourth Amendment requirements, without purpose to deter or penalize protected expression or association, do not violate the First Amendment. *See Reporters Comm.*, 593 F.2d at 1051-53; *see also id.* at 1051 (concluding that First Amendment protects activities "*subject to* the general and incidental burdens that arise from good faith enforcement of otherwise valid criminal and civil laws that are not themselves solely directed" at First Amendment conduct); *see also Gordon v. Warren Consol. Bd. of Educ.*, 706 F.2d 778, 781 n.3 (6th Cir. 1983) (collecting cases).

Here, Plaintiffs have not set forth competent evidence proving that the Government's bulk metadata or targeted content collections are (or were) aimed at curtailing any of their First Amendment expressive or associational activities, or have had any purpose other than to identify terrorist operatives and prevent terrorist attacks. *See Klayman I* Br. at 22, 25-26, *and* Am. Compl. ¶¶ 3-4, 30-33, 38-39, 57. With respect to the only targeted program at issue here—PRISM under Section 702—Plaintiffs offer no evidence that their communications have been targeted or acquired under Section 702, which is directed at non-U.S. persons located outside the United States. Accordingly, Plaintiffs' First Amendment claim has no prospect of success.

B. The Programs Plaintiffs Challenge Impose No Direct or Significant Burden on Plaintiffs' Speech or Associational Rights

Plaintiffs' contention that the metadata and content collection programs should be subjected to "exacting scrutiny" because they impose a "significant" burden on Plaintiffs' speech and associational rights, *Klayman I* Br. at 23-26; *Klayman II* Br. at 25-28, also fails as a matter of law and fact. First, as discussed above, the underlying premise of Plaintiffs' argument—that the programs expose to government scrutiny all of Plaintiffs' sensitive contacts with clients, associates, friends and relatives, as well as whistleblowers, and others with whom they might collaborate in their work—is without foundation. Plaintiffs neither allege nor offer any evidence that the metadata related to 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. Nor have Plaintiffs offered any evidence that they communicate with non-U.S. persons located overseas who could even be the targets of Section 702 collection, let alone set forth a single, concrete example that the contents of any of their communications have been targeted or incidentally collected pursuant to Section 702.

Nor have Plaintiffs set forth any competent evidence of a "chilling effect" attributable to the challenged programs that interferes with their First Amendment rights of speech or association. The evidence proffered by Plaintiffs does not show that they themselves are actually or even subjectively "chilled" by Government's activities under the challenged programs. Rather, apart from vague and conclusory assertions about the supposed "impact" of their subjective fears of surveillance on their "ability to communicate via telephone, email, and otherwise," Klayman Aff. ¶ 11; Strange Aff.¶¶ 12-20, Plaintiffs offer no evidence of actually having been chilled from communicating or associating with anyone. Further, while Plaintiffs

speculate in their brief that third-parties who regard their associations with Mr. Klayman as confidential may be "chilled" from contacting him because of the challenged programs, *see Klayman I* Br. at 26; *Klayman II* Br. at 27-28, they provide no concrete evidence to substantiate this assertion, either. Moreover, any such chill, even if shown, would be attributable to these third parties' own speculative fears of surveillance, not to conduct of the Government. *Amnesty Int'l*, 133 S. Ct. at 1152 n.7. These allegations fail to demonstrate an actual chill on speech or associational activity as required to support a First Amendment claim. *See Harris v. Holder*, 885 F. Supp. 2d 390, 400 (D.D.C. 2012) ("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.") (internal quotations omitted; alterations added); *Krieger v. DOJ*, 529 F. Supp. 2d 29, 58 (D.D.C. 2008).[35]

Nor can Plaintiffs draw any meaningful parallel between the instant matter 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, *Klayman I* Br. at 23-25; *Klayman II* Br. at 25-27, 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

[35] Indeed, while Plaintiff Klayman baldy alleges that the "NSA Program at issue in this case poses a substantial threat" to his ability to perform his political work as the Founder of Freedom Watch, Klayman Aff. ¶ 9, his affidavit details the ongoing activities of his "Reclaim America Now" movement, which includes an upcoming demonstration in Washington D.C. on November 19, 2013, *id.* ¶ 8.

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).

In contrast, Plaintiffs present no evidence that NSA's collection of communications under Section 702 targets Plaintiffs rather than non-U.S. persons located abroad. Nor do Plaintiffs allege, much less point to any evidence, that they communicate with such persons so as to make even incidental collection of their communications possible. Furthermore, the FISC orders authorizing the telephony metadata program are not based on the content of anyone's communications, and do not compel Plaintiffs to disclose, or direct anyone else, including 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*). *See* Primary Order at 3-9. Rather, 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. *Id*. 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.

Thus, even if this were a compelled-disclosure case, which it is not, 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.[36] As the Supreme Court has explained, "exacting scrutiny" applies "to regulations that

[36] For example, in *Clark v. Library of Congress*, the D.C. Circuit applied "exacting scrutiny" to a "targeted investigation of an individual based solely on the exercise of his

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 applies to government surveillance "motivated *solely by an individual's lawful beliefs or associations*") (emphasis added). Plaintiffs fall well short of this threshold. They have not alleged or submitted any evidence that the telephony metadata program is (or that the Internet metadata program was) content-based, much less directed at curtailing or punishing free expression or association. *See Klayman I* Br. at 22-26; *Klayman II* Br. at 24-28. Nor have they alleged any facts suggesting that their communications have been either targeted or incidentally collected under Section 702. Plaintiffs' failure to establish "direct and substantial" interference with their speech or associational rights brings the First Amendment inquiry—under exacting scrutiny, or any other standard—to an end. Accordingly, Plaintiffs' First Amendment claim cannot support an award of preliminary relief.

VI. PLAINTIFFS CANNOT DEMONSTRATE THAT THEY ARE LIKELY TO SUCCEED ON THEIR FIFTH AMENDMENT CLAIM

Plaintiffs assert substantive and procedural due process claims that are plainly insubstantial and should be rejected.

A. Plaintiffs' Substantive Due Process Claim Should Be Dismissed as Duplicative of Their Fourth Amendment Claim

Plaintiffs' substantive due process argument is premised on an alleged liberty interest in the privacy of their communications. *See Klayman I* Br. at 26-27; *Klayman II* Br. at 28-29. However, "[w]here a particular Amendment 'provides an explicit textual source of constitutional protection' against a particular sort of government behavior, 'that Amendment, not the more

---

associational rights," which resulted in "an extraordinary" full field investigation by the FBI. 750 F.2d 89, 93-95 (D.C. Cir. 1984). *See also Elrod v. Burns*, 427 U.S. 347, 350 (1976) (applying "exacting scrutiny" to claimed termination of public employees "solely for the reason that they were not affiliated with or sponsored by the Democratic Party").

generalized notion of "substantive due process," must be the guide for analyzing'these claims." *Albright v. Oliver*, 510 U.S. 266, 273 (1994) (quoting *Graham v. Connor*, 490 U.S. 386, 395 (1989)). Because Plaintiffs ground their substantive due process claim on privacy interests allegedly protected by the Fourth Amendment, that claim cannot serve as an independent basis for issuing a preliminary injunction. *See, e.g.*, *Elkins v. Dist. of Columbia*, 690 F.3d 554, 562 (D.C. Cir. 2012) (rejecting plaintiff's attempt to use the Fifth Amendment to challenge allegedly unlawful search and seizure); *Lyles v. Micenko*, 468 F. Supp. 2d 68, 73 n.5 (D.D.C. 2006) (Leon, J.) (refusing to analyze Fourth Amendment claim under the rubric of substantive due process).

B. Plaintiffs' Procedural Due Process Claim Is Also Meritless.

Plaintiffs also fail to state a viable procedural due process claim. They argue that the Government deprived them of the aforementioned privacy interests "the moment" the NSA "secretly collected, acquired, retained, searched, and used" information related to and contained in their communications without providing any pre-deprivation notice to Plaintiffs that would allow them to ascertain "what conduct may subject them to electronic surveillance." *Klayman I* Br. at 27; *Klayman II* Br. at 28-29. Plaintiffs cite not a single authority for the proposition that the Government must give prior notice to persons before it may gather information about their communications as part of a classified, FISC-authorized, intelligence-gathering program conducted for purposes of protecting national security. That alone should be reason enough to reject this claim as a basis for awarding extraordinary injunctive relief. But even if the Court were to entertain this claim, it would not withstand analysis.

To establish a violation of procedural due process, Plaintiffs must show that the Government deprived them of a "constitutionally protected [liberty or] property interest," and that its "procedures in doing so do not satisfy procedural due process." *Simms v. Dist. of Columbia*, 872 F. Supp. 2d 90, 95 (D.D.C. 2012); *see also Gen. Elec. Co. v. Jackson*, 610 F.3d

110, 117 (D.C. Cir. 2010). Even assuming that Plaintiffs retain a residual liberty interest in the privacy of their communications that is entitled to due-process protection above and beyond the protections already afforded by the Fourth Amendment, *see Brown v. McHugh*, No. 12-01071, --- F. Supp. 2d ---, 2013 WL 5310185, at *7 (D.D.C. Sept. 23, 2013) (Leon, J.) ("[O]nly *after* finding the deprivation of a protected interest do[es] [the Court] look to see if the [government's] procedures comport with due process.") (internal quotation omitted)), they are not "due" the pre-deprivation notice they demand.

Where protected liberty interests are implicated, the determination of what process is due requires consideration of three factors: "(1) the significance of the private party's protected interest, (2) the government's interest, and (3) the risk of erroneous deprivation and 'the probable value, if any, of the additional or substitute procedural safeguards.'" *Gen. Elec. Co.*, 610 F.3d at 117 (quoting *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976)). Due process "is not a technical conception with a fixed content unrelated to time, place and circumstances," but rather, it "is flexible and calls for such procedural protections as the particular situation demands," *Gilbert v. Homar*, 520 U.S. 924, 930 (1997) (internal quotation marks and citation omitted)), and, as relevant here, takes into account "essential national security considerations." *Gonzalez v. Freeman*, 334 F.2d 570, 580 n.21 (D.C. Cir. 1964).

Here, the Government's interest in identifying terrorist operatives and intercepting their communications for the purpose of preventing terrorist attacks is a national security concern that far outweighs any residual privacy interest that Plaintiffs may have in their communications not already protected by the Fourth Amendment, and by the same token outweighs any risk of erroneous deprivation of that interest. "[N]o governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981). The NSA's collection of

information about and the contents of telephonic and electronic communications thus promotes a governmental interest of the highest order. *See, e.g.*, *id.*; *In re Sealed Case*, 310 F.3d at 746.

Requiring the Government, however, to provide advance notice to every individual before acquiring information about his or her communications would be incompatible with the secrecy required for such intelligence-gathering programs, *see supra* at 29 & n.14, and fatal to their objectives. For example, if the Government disclosed to an individual associated with a foreign terrorist organization that his communications (and/or metadata related to them) were to be collected and subject to scrutiny by the Government, that individual, and his or her associates, could take steps to avoid detection and alter their plans, thus placing national security at greater risk.[37] Due process does not require the Government to put national security at risk in such fashion by providing communications services subscribers the process that Plaintiffs demand. *See Holder v. Humanitarian Law Project*, 130 S. Ct. 2705, 2727 (2010); *Jifry v. FAA*, 370 F.3d 1174, 1184 (D.C. Cir. 2004). Plaintiffs' Fifth Amendment claim is without merit and cannot serve as a predicate for issuing a preliminary injunction.

VII. THE BALANCE OF EQUITIES AND THE PUBLIC INTEREST REQUIRE THAT AN INJUNCTION BE DENIED

Finally, neither the public interest, nor a balancing of the equities, supports the issuance of a preliminary injunction here. Plaintiffs seek to enjoin the Government from continuing the

[37] *See Implementation*, *supra*, 109th Cong. at 65 (2005) (statement of Robert Khuzami) (explaining that advance notice "could cause conspirators to accelerate the plot to a point where authorities are less prepared to prevent it or protect American lives. Or terrorists might abandon the plot, destroying evidence and taking flight, which would hinder prevention, capture and prosecution. The plot might later resurface, at a point when we are less prepared and more vulnerable."); Shea Decl. ¶ 49. *See also, e.g.*, *Calero-Toledo v. Pearson Yacht Leasing Co.*, 416 U.S. 663, 679 (1974) (dispensing with pre-deprivation notice or hearing when exigent circumstances exist and the government demonstrates a "pressing need for prompt action"); *Global Relief Found., Inc. v. O'Neill*, 207 F. Supp. 2d 779, 803 (N.D. Ill. 2002) ("Due to the exigencies of national security and foreign policy considerations, the Executive Branch historically has not provided pre-deprivation notice in sanctions programs under [the International Emergency Economic Powers Act].").

programs implicated by their allegations,[38] to bar them from collecting information about Plaintiffs' communications, to require them to segregate and destroy all such records, and to prohibit the Government Defendants from querying metadata collected under these programs using Plaintiffs' identifiers. *See Klayman I* Br. at 30-31; *Klayman II* Br. at 32-33.

The Court must balance Plaintiffs' asserted irreparable harm if injunctive relief is denied against the harm to the public interest if it is granted. *See Winter v. NRDC*, 555 U.S. 7, 25 (2008). Whereas Plaintiffs failed to demonstrate irreparable harm, *see supra* at 25-26, the public has a strong interest in continuing the programs involving the bulk collection of telephony metadata and the targeted collection of communications under Section 702. The former program "is a valuable source of intelligence for the FBI that is relevant to FBI-authorized international terrorism investigations," Holley Decl. ¶ 22, and the latter program "has produced and continues to produce significant intelligence that is vital to protect the nation against international terrorism and other threats." Letter from DNI James R. Clapper and Attorney General Eric Holder to the Honorable John Boehner, Harry Reid, Nancy Pelosi, and Mitch McConnell (Feb. 2, 2012) (Exh. T, hereto). Courts accord great deference to the professional judgment of intelligence officials regarding counter-terrorism matters, and they are properly reluctant to interfere with those judgments. *Humanitarian Law Project*, 130 S. Ct. at 2727 (according deference to Executive judgments on national security). Given that "[e]veryone agrees that the Government's interest in combating terrorism is an urgent objective of the highest order," *id*. at 2724, and that the Court must be particularly mindful of an injunction's "consequent adverse impact on the public interest

[38] The pen/trap program involving the bulk collection of Internet metadata need not be analyzed here because the Government has, for operational and resource reasons, terminated this collection in 2011. *See* Clapper Letter dated July 25, 2013, Exh. J, *supra*, at 3.

in national defense," *Winter*, 555 U.S. at 24, the public interest and the balance of the equities weigh strongly against enjoining the challenged programs.[39]

The balance of the equities also strongly favors denying Plaintiffs' demand that the Government Defendants segregate and destroy and records of their communications (if any have been collected). Even if the Government Defendants possessed information concerning Plaintiffs' communications, segregation of that information would be "extraordinarily burdensome," could take six months to implement, and could ultimately have a degrading effect on the utility of the program if an injunction in this case precipitated successful requests for such relief by other litigants. *See* Shea Decl. ¶ 65. Plaintiffs' demand that the Government Defendants destroy any such information now would essentially and improperly give them full relief on the merits at this preliminary stage. *See Dorfmann v. Boozer*, 414 F.2d 1168, 1173 n.13 (D.C. Cir. 1969) ("[A] preliminary injunction should not work to give a party essentially the full relief he seeks on the merits."); *Bradshaw v. Veneman*, 338 F. Supp. 2d 139, 144–45 (D.D.C. 2004) (Friedman, J.) ("[A] hurried resolution in favor of plaintiffs is not the purpose of temporary or preliminary injunctive relief.").

CONCLUSION

For the reasons stated above, Plaintiffs' motions for preliminary injunctions should be denied.

---

[39] While the Government Defendants acknowledge the public interest in ensuring that the government agencies comply with the law, as argued by Plaintiffs, *see Klayman I* Br. at 29-30; *Klayman II* Br. at 32, this interest has been and is being vindicated through the statutory framework for Sections 215 and 702 that involves stringent supervision and oversight by all three branches. *See* 50 U.S.C. § 1861(a), (b) (Executive must apply to the FISC for an order requiring the production of tangible things under Section 215), *id*. § 1861(g) (Executive minimization procedures); Letter from Ronald Weich to Rep. Silvestre Reyes (Dec. 14, 2009) (sharing information about the bulk collection of telephony metadata with Congress); *see also* 50 U.S.C. § 1881a(d), (e), (i) (judicial review of Section 702 Executive certifications, as well as targeting and minimization procedures); *id*. § 1881a(l) (semi-annual compliance reports by Executive to the FISC and to Congress).

Dated: November 12, 2013

Respectfully Submitted,

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel
james.gilligan@usdoj.gov
MARCIA BERMAN
Senior Trial Counsel
BRYAN DEARINGER
RODNEY PATTON
Trial Attorneys
U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470

Counsel for the Government Defendants