STUART F. DELERY
Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
BRYAN DEARINGER
Trial Attorney
RODNEY PATTON
Trial Attorney
U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
james.gilligan@usdoj.gov

Attorneys for the Government Defs. in their Official Capacity

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

FIRST UNITARIAN CHURCH OF LOS ANGELES, *et al.*,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Case No. 3:13-cv-03287-JSW

GOVERNMENT DEFENDANTS' REPLY IN SUPPORT OF THEIR MOTION TO DISMISS

Date: April 25, 2014
Time: 9:00 a.m.
Courtroom 11, 19th Floor
The Honorable Jeffrey S. White

INTRODUCTION

In support of their motion to dismiss, the Government Defendants demonstrated that Plaintiffs' claims are jurisdictionally barred, and that the telephony metadata program is both authorized under Section 215 and constitutional. Plaintiffs' opposition brief does nothing to alter these conclusions, and their First Amended Complaint must be dismissed as a matter of law.

ARGUMENT

I. PLAINTIFFS HAVE NOT ESTABLISHED THEIR STANDING TO SUE.

Plaintiffs must "demonstrate standing for each claim [they] seek[] to press," *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006). Plaintiffs' asserted injuries cannot support standing as to any of their claims because they are too speculative, not fairly traceable to the actual operation of the telephony metadata program,[1] and arise, instead, from speculative fears that the NSA has reviewed, or will in the future review, metadata related to their calls in order to identify them (or others) with particular groups or causes. *See* Gov't Mot. at 11-15.

Plaintiffs argue in response, Pls.' Opp. at 2-5, 16-17, and erroneously so, that they have standing because the Government has "publicly admitted" the "actual collection of their phone records" (*id.* at 4) and that "collection alone" (*id.* at 17) is sufficient to confer standing as to all their claims. As an initial matter, the Government has acknowledged the participation in the program of only a single specific provider for the duration of the now-expired April 19, 2013, Secondary Order. Only three of the plaintiff organizations allege that they have been subscribers to this provider's services, and even they do not specify when. *See* Gov't Mot. at 14 n.5.[2]

[1] Plaintiffs are consequently wrong in claiming that the "government only challenges . . . whether plaintiffs have adequately alleged injury in fact" and that there is "no dispute" that Plaintiffs "have adequately alleged causation." Pls.' Opp. at 2 n.2; *see* Gov't Mot. at 11-15.

[2] Nor can Plaintiffs rely on speculation about the program's scope to infer that metadata associated with their calls must have been collected. *See* Pls.' Opp. at 3. While the Government has acknowledged that the telephony metadata program is broad in scope and involves the aggregation of an historical repository of data collected from more than one provider, the Government has not stated, nor is it correct, that the program captures information about all—or even virtually all—telephone calls to, from, or within the United States. Supp. Decl. of Teresa H. Shea (Supp. Shea Decl.) ¶ 7 (filed herewith); *see also* Aug. 29, 2013 FISC Op. at 4 n.5 ("production of all call detail records of all persons in the United States has never occurred under this program."). Contrary to Plaintiffs' suggestions, Pls.' Opp. at 4-5, in ruling on a motion to dismiss the Court can "resolve factual disputes concerning the existence of jurisdiction," *McCarthy v. United States*, 850 F.2d 558, 560 (9th Cir. 1988), and require Plaintiffs to supply "further particularized allegations of fact." *Warth v. Seldin*, 422 U.S. 490, 501-02 (1975).

Even if Plaintiffs could establish that metadata associated with their calls have been collected, they cite no support for their theory that "collection alone" (Pls.' Opp. at 17) of these third-party business records, without review of their contents, is sufficient to show "invasion of a legally protected interest," *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992), under the Fourth or Fifth Amendment, or otherwise;[3] and the idea is cast into doubt by substantial authority.[4] Absent queries of the data to which any records collected of Plaintiffs' calls would be responsive[5]—and Plaintiffs have alleged none—NSA analysts cannot even review records of Plaintiffs' calls, much less glean information about Plaintiffs' contacts or associations.[6]

Nor can mere collection of metadata associated with Plaintiffs' calls create standing under the First Amendment without a demonstrated infringement of their free speech or association that is traceable to the actual operation of the program. Gov't Mot. at 4-8, 12-15. As

[3] Plaintiffs assert that the Stored Communications Act bestows rights upon them, the invasion of which confers standing, *see* Pls' Opp. at 17, but an invasion of statutory rights, even if shown, does not confer standing to raise constitutional claims. *See Jewel v. NSA*, 673 F.3d 902, 908-09 (9th Cir. 2011) (explaining that standing to assert constitutional claim requires invasion of rights protected by the applicable constitutional provision; analyzing statutorily created rights separately). And even if Plaintiffs had demonstrated standing to raise the one statutory claim they press, "congressional preclusion of review" of their statutory claim, *see* Gov't Mot. at 15-20, *infra* at 3-10, still deprives the Court of jurisdiction to consider it. *Block v. Cmty. Nutrition Inst.*, 467 U.S. 340, 353 n.4 (1984) (preclusion "is in effect jurisdictional").

[4] *See Horton v. California*, 496 U.S. 128, 142 n.11 (1990) (Government acquisition of an item without examining its contents "does not compromise the interest in preserving the privacy of its contents"); *United States v. VanLeeuwen*, 397 U.S. 249, 252-53 (1970) (privacy interest in defendant's detained first-class mail "was not disturbed or invaded" until the government opened it); *United States v. Licata*, 761 F.2d 537, 541 (9th Cir. 1985) (seizure of package "affects only the owner's possessory interests and not the privacy interests vested in the contents").

[5] In connection with a transition of the telephony metadata program, the President recently ordered, and the FISC has adopted, changes to the program that (1) require the Government, in addition to satisfying the "reasonable, articulable suspicion" standard, to obtain permission from the FISC to use a proposed selection term as a "seed" to query the telephony metadata, and (2) limit the results of each query to metadata that are within two, rather than three, "hops" of the approved seed used to conduct the query. *See* Supp. Shea Decl. ¶¶ 4-6.

[6] Contrary to Plaintiffs' arguments, *see* Pls.' Opp. at 3, 4, 17, *Jewel v. NSA*, 673 F.3d 902 (9th Cir. 2011) does not support their standing. There it was found that plaintiffs had sufficiently alleged that they were personally subjected to alleged NSA "dragnet" surveillance of both the content and records of telephone and Internet communications "of practically every American" to confer Fourth Amendment standing at the pleading stage. *Id.* at 906, 908-10. This case involves alleged collection of non-content third-party business records, which does not implicate the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 735, 742-46 (1979); *see infra* at 11-15. Absent an alleged *invasion* of a legally protected interest, *Defenders of Wildlife*, 504 U.S. at 560, standing is not established at the pleading stage and thus *Jewel* is distinguishable. Moreover, Plaintiffs cannot rely on mere allegations when seeking summary judgment. *Id.* at 561.

recently held by the court in *ACLU v. Clapper*, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013), "speculative fear" that "telephony metadata related to . . . calls" would be "queried or reviewed" and the "identities of the telephone subscribers determined . . . 'relies on a highly attenuated chain of possibilities,'" which is "'insufficient to create standing" for a First Amendment claim. *Id.* at *7, 24 (quoting *Amnesty Int'l USA v. Clapper*, 133 S. Ct. 1138, 1148, 1152).[7]

II. PLAINTIFFS' STATUTORY CLAIM (COUNT IV) MUST BE DISMISSED.

A. Count IV Is Precluded and Thus Barred by Sovereign Immunity.

The Court lacks jurisdiction over Count IV of the Amended Complaint, an APA claim that the telephony metadata program exceeds the authority conferred by Section 215,[8] because application of the APA's waiver of sovereign immunity, 5 U.S.C. § 702, is impliedly precluded by both Section 215 and section 223 of the USA-PATRIOT Act. Gov't Mot. at 15-20. That conclusion has also been reached by two district courts presented with the same statutory attack on the program that Plaintiffs attempt to mount here, *ACLU*, 2013 WL 6819708, at *9-13; *Klayman v. Obama*, 2013 WL 6571596, at *9-12 (D.D.C. Dec. 16, 2013), and is compelled by this Court's reasoning in *Jewel v. NSA*, 2013 WL 3829405, at *12 (N.D. Cal. July 23, 2013).

Plaintiffs argue that the APA's waiver of sovereign immunity applies to their statutory claim because 18 U.S.C. § 2712(d) expressly provides that a damages claim thereunder shall be the "exclusive" remedy for violations of the FISA provisions "within its purview." Therefore,

---

[7] Plaintiffs' reliance (Pls.' Opp. at 3) on *Presbyterian Church (USA) v. United States*, 870 F.2d 518 (9th Cir. 1989), is misplaced. In that case federal agents entered four churches without a warrant and "surreptitiously tape recorded several services." *Id.* at 520. When those surveillance activities were publicized, the four churches claimed that congregants at their churches were "chilled" from participating in church activities (evidenced by documented withdrawal of members), which inhibited the churches' ministries. *See id.* at 521-22. Here, in contrast, there is no allegation (much less any evidentiary showing) that telephony metadata revealing associations between Plaintiffs and others—the First Amendment protected activity here—have ever been seen or reviewed by NSA analysts. The case is therefore inapposite.

[8] Plaintiffs' argument that Count IV is a claim "for damages for violations of the Stored Communications Act[ ]" [SCA], for which 18 U.S.C. § 2712 "expressly waives sovereign immunity," Pls.' Opp. at 17, is specious. As announced by its caption, Count IV is a claim seeking injunctive and other equitable relief, Am. Compl. ¶ 108, based on alleged violation of Section 215, *id.* ¶¶ 104-05, for which Plaintiffs expressly invoke APA § 702 as the applicable waiver of sovereign immunity, *id.* ¶ 106. Count IV makes no reference to money damages, the SCA, or § 2712. Even if Plaintiffs had purported to plead a claim for damages under the SCA, the Court would still lack jurisdiction over Count IV, because they admittedly have not complied with § 2712's exhaustion requirement. 18 U.S.C. § 2712(b)(1); *see* Pls.' Opp. at 18 n.23.

say Plaintiffs, it cannot be taken to impliedly preclude injunctive relief for alleged violations of other provisions such as Section 215. Pls.' Opp. at 19-20 & n.24. But express preclusion of certain FISA-based claims does not foreclose implied preclusion of other claims not specified by § 2712(d). Here, preclusion follows from Congress's decision to provide a damages remedy for misuses of information obtained under particular provisions of FISA—not including Section 215—while at the same time expressly excluding the United States from liability under the SCA's cause of action for injunctive relief, 18 U.S.C. § 2707. *See* Gov't Mot. at 17. Indeed, that is the conclusion this Court reached in *Jewel*, in the face of the same argument advanced by Plaintiffs here. *See* 2013 WL 3829405, at *10, 12 (rejecting argument that the plaintiffs' claim under 50 U.S.C. § 1809 was not precluded because they had brought "a different claim, seeking different relief" under a provision of FISA not listed in § 2712).[9]

Plaintiffs also fail to overcome the separate bar to their statutory claim erected by Section 215. They do not contest the reasoning that Section 215 impliedly precludes APA relief by establishing a secret and expeditious process for obtaining (and challenging) production orders that involves only the Government and the recipient. *See ACLU*, 2013 WL 6819708, at *12; *Klayman*, 2013 WL 6571596, at *10-11; Gov't Mot. at 18-19. Rather, they argue that subsection (f), 50 U.S.C. § 1861(f)—which allows recipients to petition the FISC to set aside nondisclosure orders imposed in connection with production orders—reflects an intent by Congress to permit third parties to challenge production orders that "become known to them." Pls.' Opp. at 21.

To the contrary, subsection (f) places strict limitations on recipient challenges to Section 215 nondisclosure orders, which dispel any notion that Congress meant to pave the way for third-party challenges to production orders once they "become known." First, subsection (f) permits only recipients to petition the FISC to set aside nondisclosure orders as recipients may see fit to do or not in their own interest, without regard for the interests of others who might desire to contest production orders. 50 U.S.C. § 1861(f)(2)(A)(i). Second, and perhaps most significantly, Congress barred even recipients from seeking to set aside nondisclosure orders until at least "1 year after the date" of the corresponding production orders, *id.*, meaning a

[9] The court in *Klayman* also rejected the argument that FISA claims not falling "within the purview" of § 2712(a) cannot be impliedly precluded, 2013 WL 6571596, at *12 n.30.

recipient ordinarily would have complied with an order long before its existence could possibly "become known"—at least through the process Congress envisioned—to any third party who might want to challenge production of the records in question.

Third, a recipient petition to set aside a nondisclosure order may be granted only if the FISC finds "no reason to believe that disclosure may endanger the national security …, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person." *Id.* § 1861(f)(2)(C)(i), (ii). That extremely high hurdle also reflects an expectation by Congress that public disclosure of production orders would be a rarity, not a routine path to collateral litigation over compliance with Section 215's requirements. Finally, if Congress had meant for third parties to enjoy a right to review of production orders after their disclosure under subsection (f), then it stands to reason that Congress would have provided for such review in the FISC, as it so provided for recipients. *Cf. Cmty. Nutrition Inst.*, 467 U.S. at 347. Thus, contrary to Plaintiffs' argument, subsection (f) reinforces the conclusion that "Congress simply did not intend" for third parties such as Plaintiffs "to be relied upon to challenge disregard" of Section 215's requirements. *Id.* at 351.

Plaintiffs' arguments get no boost from *Sackett v. EPA*, 132 S. Ct. 1367 (2012). *See* Pls.' Opp. at 21, 22. *Sackett* merely held that one provision of an act authorizing judicial review of one type of agency order did not preclude *all* review of another type of order, even at the behest of recipients of such orders. *Id.* at 1373. That result has no relevance here, where Congress has provided a means for recipients to obtain review (in the FISC) of the same type of order that Plaintiffs seek to challenge, but did not extend that same right of review to third parties. The preclusion analysis here is instead squarely controlled by the principle articulated in *Community Nutrition Institute*, that where "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." 467 U.S. at 349.[10]

[10] Plaintiffs' suggestion that preclusion turns on the presence of administrative exhaustion requirements in the statutory scheme, Pls.' Opp. at 21-22, is also not well taken. *See Community Nutrition Inst.*, 467 U.S. at 347 (finding express inclusion of certain classes of persons in the regulatory process but not others was "sufficient reason" alone to conclude that Congress intended to foreclose the latter's participation). In any event, allowing third-party challenges to Section 215 orders (especially without observance of subsection (f)'s one-year waiting period)

B. Bulk Collection of Telephony Metadata Is Authorized Under Section 215.

1. The metadata are relevant to FBI counter-terrorism investigations.

Plaintiffs' statutory claim should also be dismissed on the merits because the NSA's bulk collection of telephony metadata falls well within the scope of authority conferred by Section 215. Gov't Mot. at 20-32. Plaintiffs' principal contention to the contrary, that there are no "reasonable grounds to believe," 50 U.S.C. § 1861(b)(1)(A), that bulk telephony metadata are relevant to authorized counter-terrorism investigations, Pls.' Opp. at 22-25, lacks merit. As held by the FISC and now the court in *ACLU*, the NSA's bulk collection of telephony metadata meets Section 215's expansive standard of relevance because 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, *see ACLU*, 2013 WL 6819708, at *17-18; Aug. 29 FISC Op. at 18-23. Congress ratified that conclusion by extending Section 215's authorization, without substantive change, in 2010 and 2011. *Id.* at 23-28; *see also ACLU*, 2013 WL 6819708, at *15-16; Oct. 11 FISC Mem. at 3; Gov't Mot. at 24-25.

Seeking to show that the FISC lacked a basis for repeatedly reaching this conclusion—now thirty-six times, by fifteen different judges, over nearly eight years, Supp. Shea Decl. ¶ 3—Plaintiffs first argue that tying the concept of relevance "to the government's use of new and sophisticated analytical tools" represents a "significant change" and "shift in the definition of the term." Pls.' Opp. at 23. That assertion ignores the evolving role that technology has played in government investigations at least since the advent, generations ago, of fingerprint analysis. *See Maryland v. King*, 133 S. Ct. 1958, 1977 (2013). Over the past century, various types of evidence have become relevant to government investigations because of advances in analytical capabilities that make it possible to derive useful information that could not be obtained before.[11]

---

would be just as disruptive to the efficiency of the process Congress envisioned under Section 215 for obtaining information relevant to FBI counter-terrorism investigations, *see* Gov't Mot. at 18-19, as consumer suits would have been to the "delicate administrative scheme" at issue in *Community Nutrition Institute*, 467 U.S. at 347-48.

[11] For example, an interstate database of DNA samples can be relevant to criminal investigations because of "sophisticated analytical tools" that "make[ ] it possible to determine whether a biological tissue matches a suspect with near certainty." *See, e.g.*, *King*, 133 S. Ct. at 1967-68. The entirety of a person's computer hard drive may be relevant to an investigation because of powerful computer forensic tools "capable of unlocking password-protected files,

By the same token, bulk telephony metadata fall within the accepted understanding of relevance in the investigatory context because "'bulk collection is necessary for NSA to employ tools that are likely to generate useful investigative leads to help identify and track terrorist operatives.'" Aug. 29, 2013 FISC Op. at 20-23 (citation omitted); *ACLU*, 2013 WL 6819708 at *17 (same).

Plaintiffs again express concern about the "potential reach" of this accepted understanding of relevance, Pls.' Opp. at 23; *see* Pls.' Mem. at 9, but the fact that "relevance" cannot be reduced to a cut-and-dry formula, and must be judged "in relation to the nature, purpose, and scope of the inquiry" at hand, was recognized and accepted by the Supreme Court nearly 70 years ago. *See Okla. Press Pub. Co. v. Walling*, 327 U.S. 186, 209 (1946). That is not to say that bulk collection of telephony metadata raises no legitimate concerns about Americans' personal privacy. But as the FISC and the court in *ACLU* observed, "significant post-production minimization procedures" limit access to and dissemination of U.S.-person information derived from the data to legitimate foreign-intelligence purposes. Aug. 29, 2013 FISC Op. at 23; *ACLU*, 6819708, at *17; *see* Gov't Mot. at 6-8. Plaintiffs' ill-defined fears of Government overreach, whether involving this program, or some other intelligence program in the future, supply no valid basis for second-guessing the relevance determinations the FISC has consistently made in authorizing the telephony metadata program. *See* Gov't Mot. at 28-29.[12]

---

restoring deleted material, and retrieving images viewed on websites." *See United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc).

[12] Plaintiffs argue that the FISC's relevance determinations are entitled to no deference because they are not the product of an adversary process. Pls.' Opp. at 26-27. This argument is misguided. The FISC is an Article III court whose ability to provide responsible oversight of the Government's surveillance activities is not open to question. *United States v. Cavanagh*, 807 F.2d 787, 790-91 (9th Cir. 1987). The FISC issues orders under Title I of FISA without conducting adversary proceedings, yet judicial review of FISA orders is "deferential," involving only "minimal scrutiny by the courts." *United States v. Abu-Jihaad*, 630 F.3d 102, 130 (2d Cir. 2010). The relevance of information sought under grand jury or administrative subpoenas, which the Government may issue without any prior judicial authorization, is also subject only to the most deferential review by the courts. *See* Gov't Mot. at 26-27 & n.22. Plaintiffs' related accusation, that the Government has "stretch[ed] the truth" in its filings before the FISC, Pls.' Opp. at 26-27, is baseless. Their claim that the Government asserted that bulk telephony metadata are "vital to the government's ability to protect the nation from attack" overlooks the distinction between the necessity of the data to effective use of NSA analytic tools, and the value of the resulting investigative leads to the FBI's counter-terrorism mission. The distinction has not been lost on the FISC, whose understanding of the program's importance is entirely consistent with the Government's representations to this Court. *Compare* Aug. 29, 2013 FISC Op. at 20 ("'finding of relevance most crucially depend[s] on the conclusion that bulk collection is *necessary for NSA to employ tools* that are likely to generate *useful investigative leads* to help

Again seeking to depict the program as a "fishing expedition," Plaintiffs assert that the FISC has (on thirty-six occasions) disregarded Section 215's requirement that the items sought be relevant to "an authorized investigation," and not to counter-terrorism generally. Pls.' Opp. at 23-25. This argument is counter-factual. The FBI seeks the production of call-detail records for purposes of investigations "that concern specified terrorist organizations" identified in each application submitted to the FISC. Skule Decl. ¶ 10; *see* Gov't Mot. at 5. The FISC's orders are expressly predicated on findings that the data are relevant to counter-terrorism investigations "being conducted" by the FBI. *See* Primary Order at 2. The orders permit queries of the data using only those identifiers that are reasonably suspected of being linked with one or more of the specific terrorist organizations that are the subjects of the identified FBI investigations. *See id.* ¶ 3(C)(i) at 7.[13] It is of no moment that the data are sought for purposes of multiple investigations rather than a single "authorized investigation," Pls.' Opp. at 23-24. *See* 1 U.S.C. § 1 ("[i]n determining the meaning of any Act of Congress, unless the context indicates otherwise, words importing the singular include [the plural].").[14]

As the FISC has found, reason and experience demonstrate that information revealing unknown domestic operatives of foreign terrorist organizations may be found within the bulk telephony metadata the NSA obtains, information that has proven valuable to the FBI's ongoing investigations of these organizations, and its efforts to thwart their plans. Aug. 29 FISC Opp. at

---

identify and track terrorist operatives'") (emphasis added) *with* Skule Decl. ¶¶ 8-9, 19 (the program is "an important tool in counter-terrorism investigation"); Shea Decl. ¶ 12.

[13] *See also* Shea Decl. ¶ 20; *ACLU*, 6819708, at *5; Aug. 29 FISC Op. at 4 ("sole purpose of this production is to obtain foreign intelligence information in support of … individual authorized investigations"); *id* at 19 (the Government can meet the standard if it can "demonstrate reasonable grounds to believe that the information sought to be produced has some bearing *on its investigations of the identified international terrorist organizations*") (emphasis added). The fact that the data are also used by the NSA to identify unknown persons who may be affiliated with terrorist organizations under investigation, so the FBI may investigate whether these persons are in fact linked to the targeted organizations, *see* Cohn Decl. Exh A at 15__ (quoted by Pls.' Opp. at 24), does not reflect an inversion of Section 215's purposes, but a legitimate use of the data to advance existing investigations of the targeted organizations.

[14] In any event, the FBI could submit separate applications seeking separate orders for bulk production of telephony metadata for purposes of each ongoing investigation of a foreign terrorist organization; but nothing in the text of Section 215 prohibits the FBI from sparing itself, the FISC, and telecommunications service providers that unnecessary administrative burden by combining its requests into a single application for a single primary order.

20, 21; *see* Gov't Mot. at 28. Plaintiffs have made no showing to the contrary, and their repeated efforts to disparage the program as a "fishing expedition" again fail.[15]

2. The bulk collection of telephony metadata under Section 215 is not barred by the Stored Communications Act.

Plaintiffs' argument that collection of telephony metadata under authority of Section 215 is prohibited by the SCA was long ago and properly rejected by the FISC, *see* Gov't Mot. at 30-31 & Exh. R, and recently again in *ACLU*, 2013 WL 6819708, at *13-14.[16] Subparagraph (c)(2)(D) of Section 215, 50 U.S.C. § 1861(c)(2)(D), provides that the Government may obtain an order under Section 215 for production of any type of record that can be obtained by "any other order" of a U.S. court directing the production of records or tangible things. Thus, by operation of the express terms of subparagraph (c)(2)(D), telephony metadata can be obtained under Section 215 because the SCA provides, in 18 U.S.C. § 2703(c)(1)(B), that such records can be obtained pursuant to a court order under § 2703(d). Plaintiffs misapprehend the interplay between the two statutes. *See* Pls.' Opp. at 17-19. The point is not that a Section 215 order should be treated as the equivalent of an order under § 2703(d) (which applies only to criminal investigations), or as an implied exception to the SCA's general prohibition against disclosure of customer communication records to the government. Rather, the plain language of subparagraph (c)(2)(D) itself creates an express exception for Section 215 orders, providing that so long as the

[15] Congress legislatively ratified the construction of Section 215 as authorizing bulk collection of telephony metadata, Gov't Mot. at 24-25; Aug. 19, 2013 FISC Op. at 23-28, a conclusion also reached in *ACLU*, 2013 WL 6819708, at *15-16. Plaintiffs continue to insist that "ratification can be found only … where the specific interpretation of the statute was broad and unquestioned," Pls.' Opp. at 31-32, but the cases they cite stand only for the unremarkable proposition that ratification cannot be found where there is no "settled judicial construction" for Congress to ratify, *e.g.*, *United States v. Powell*, 379 U.S. 48, 55 n.13 (1964); *see Jama v. ICE*, 543 U.S. 335, 349-53 (2005), or where an agency interpretation is irreconcilable with a statute's plain language, *SEC v. Sloan*, 436 U.S. 103, 110-12, 120-21 (1978). Here, far from being an elephant hidden in a mouse hole, *see* Pls.' Opp. at 22, Congress was apprised of the settled understanding of Section 215 reached by the Executive Branch *and* the FISC (the only court with original jurisdiction over the subject matter). That is more than sufficient under Supreme Court precedent for application of the legislative ratification doctrine. *See* Gov't Mot. at 25 & n.20; *see also Shapiro v. United States*, 335 U.S. 1, 12 n.13 (1948) (cited with approval in *Powell*).

[16] Plaintiffs dispute that it would be anomalous (as found by both courts) to prohibit acquisition of telephony metadata under Section 215 while permitting it through national security letters (NSLs), on the premise that NSLs can only be used for targeted, not "mass" collection. Pls' Opp. at 29. They overlook, however, that under their reading the SCA would prohibit even targeted collection of telephony metadata under Section 215. Hence, the anomaly remains.

records in question could be obtained by "any other" court order—such as an order under § 2703(d)—then they can also be obtained via an order issued under Section 215. As Plaintiffs observe, subparagraph (c)(2)(D) acts as a limit on the types of records that can be obtained under Section 215, but so long as the records sought fall within this "outer boundary," Pls.' Mem. at 7, the Government's statutory authority to obtain them cannot be doubted.[17]

3. Call-detail records are "tangible things" and "documents" within the meaning of Section 215.

Plaintiffs continue to argue that call-detail records are not "tangible things" or "documents" within the meaning of Section 215, 50 U.S.C. § 1861(a)(1) (authorizing collection of "tangible things (including books, records, papers, documents, and other items)"), yet they do not contest that electronic records fall within the accepted understanding of the terms "tangible" (materially existent or real) and "document" (a computer file containing data) at the time Section 215 was enacted. *See* Gov't Mot. at 31-32; Pls.' Opp. at 29-30. Instead they invoke the maxim of statutory construction that the term "including," used to introduce a parenthetical phrase, usually signifies illustration, not expansion, of the general term that precedes it. Pls.' Opp. at 30. But that observation only proves the Government Defendants' point. Inasmuch as Section 215's use of the term "documents," including by definition computer data files, is meant as an example of "tangible things" obtainable under Section 215, it confirms (consistent with the compelling importance of the statute's purposes, and the digital age in which we live) that materially existent items such as electronic records fall within its ambit.[18] Count IV should be dismissed.

---

[17] Plaintiffs also observe that subsection 2703(d) requires a showing based on "specific and articulable facts" that the records sought are "relevant" and "material" to a criminal investigation. Pls.' Opp. at 28. Section 215 makes clear, however, that so long as the type of record to be produced falls within the scope of subparagraph (c)(2)(D), then the Government need not meet the standard another statute might impose for obtaining the records, but may acquire them if the Government's application "meets the requirements" for production under Section 215 itself, including its relatively undemanding relevance requirement. 50 U.S.C. § 1861(c)(1). Indeed, as noted by the FISC, Congress adopted a lower threshold for acquisition of records under Section 215 than under the SCA given the different purposes served by the two statutes—twice rejecting higher thresholds of specificity and materiality for collection of records under Section 215. Aug. 29 FISC Op. at 12-14; *see* Gov't Mot. at 28 n.23.

[18] Plaintiffs also argue that production of the data to the NSA is inconsistent with Section 215 because the statute contemplates production to the FBI (although it does not so specify, *see* 50 U.S.C. § 1861(a)(1)). Pls.' Opp. at 25. The statute expressly provides, however, that the FBI may disseminate information obtained under a production order "consistent with the need of the United States to obtain, *produce*, and disseminate foreign intelligence information." 50 U.S.C.

III. PLAINTIFFS' FOURTH AMENDMENT CLAIM FAILS AS A MATTER OF LAW

Smith v. Maryland, 442 U.S. 735 (1979), establishes that Plaintiffs have no reasonable expectation of privacy in telephony metadata, and is fatal to their Fourth Amendment claim. *See* Gov't Mot. at 33-36. Recognizing this, Plaintiffs try to distinguish *Smith* and point the Court instead to the concurrences in *United States v. Jones*, 132 S. Ct. 945 (2013). *See* Pls.' Opp. at 36-38. They also seek to avoid *Smith* by arguing that subsequently enacted statutes create expectations of privacy in telephone records that are protected by the Fourth Amendment, *see id.* at 33-35, and assuming that metadata collection constitutes a search, they contest the reasonableness of that search. These arguments are meritless.

A. *Smith* Controls Here, Not the Concurrences in *Jones*.

Plaintiffs' attempts to distinguish *Smith* from this case are unavailing; the differences they cite are immaterial to *Smith*'s holding that there is no reasonable expectation of privacy in telephony data voluntarily provided to third parties. *See* Gov't Mot. at 33-36. First, Plaintiffs' attempt to distinguish *Smith* based on the scope of the program challenged here, Pls.' Opp. at 37, fails because Fourth Amendment rights are personal, *see* Gov't Mot. at 35-36, and even the "collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search." *ACLU*, 2013 WL 6819708, at *22.

Second, Plaintiffs argue that accumulating five years of telephony metadata (rather than the two weeks of data collected in *Smith*) gives the NSA "the capability to build a deeply invasive associational dossier" on each person as to whose calls data have been collected. Pls.' Opp. at 33, 37. The same concern, that such data could "reveal the most intimate details of a person's life," was equally present and raised by the dissent in *Smith*, 442 U.S. at 748 (Stewart, J., dissenting), yet the Court still found no reasonable expectation of privacy. *Id.* at 741-42. Moreover, even if Plaintiffs had a hypothetical expectation of privacy in telephony metadata, they have made no showing that this asserted interest has been invaded through actual review of

§ 1861(g)(2)(A) (emphasis added), (h). Hence, were the data provided to the FBI instead of the NSA, the FBI could immediately make the data available to the NSA, consistent with applicable minimization procedures, to "produce" foreign intelligence information from the raw data, as the NSA does now. Nothing in the statute prohibits elimination of such a technically complex, time-consuming, and costly intermediate step by production of the data directly to the NSA.

any data pertaining to their calls, much less compilation of "dossier[s]" about them by NSA analysts. *See* Gov't Mot. at 4-8.[19]

Third, Plaintiffs also try to distinguish *Smith* because telephone usage has changed dramatically since *Smith* was decided. *See* Pls.' Opp. at 37. As the *ACLU* court recognized, however, the nature of telephony metadata has not: "Telephones have far more versatility now than when *Smith* was decided . . . [and] there are more calls[, but this] does not undermine the Supreme Court's finding that a person has no subjective expectation of privacy in telephony metadata." *ACLU*, 2013 WL 6819708, at *22.

Fourth, Plaintiffs argue that *Smith* is distinguishable because the pen register there recorded only numbers dialed, not "whether the call was completed, its duration, and other information." Pls.' Opp. at 36, 37. *Smith*'s rationale applies equally to these types of metadata because either Plaintiffs turn over that information voluntarily or it is information collected or generated by phone companies themselves. *See* Primary Order at 3 n.1; 442 U.S. at 742-44.

Finally, Plaintiffs attempt to distinguish *Smith* because the defendant there was a criminal suspect, whereas the challenged program here collects metadata without individualized suspicion. *See* Pls.' Opp. at 37. Individualized suspicion, however, has no bearing on whether a Fourth Amendment search occurred, *see Smith*, 442 U.S. at 742; *ACLU*, 2013 WL 6819708, at *20, but is instead part of the reasonableness analysis conducted *after* a court finds that a search has occurred. *See, e.g.*, *Klayman*, 2013 WL 6571596, at *23.

Instead of following binding precedent in *Smith*, Plaintiffs suggest that the Court look to two concurring opinions in *Jones* to find that a search occurred here, *see* Pls.' Opp. at 37-38. In *Jones*, law enforcement officers attached a GPS device to a known suspect's vehicle for 28 days

[19] Plaintiffs claim that the Government has "repeatedly searched" metadata of their calls through electronic queries of the database, even when those queries retrieve no records about their calls. *See* Pls.' Opp. at 33; Am. Compl. ¶¶ 69, 71. But queries of the database provide NSA analysts with no information about the communications in which a subscriber has engaged unless they fall within one to two (previously three) "hops" of an identifier reasonably suspected of being linked with a foreign terrorist organization. *See* Gov't Mot. at 6-7. Queries that return no records of Plaintiffs' calls cannot be considered Fourth Amendment searches. *See United States v. Place*, 462 U.S. 696, 707 (1983) (sniff of luggage by narcotics detection dog not a search because privacy of contents not disturbed); *see also United States v. Jacobsen*, 466 U.S. 109, 123 (1984) ("A chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy.").

to track his movements, *Jones*, 132 S. Ct. at 948. Although the Court's holding was that a search had occurred because the government attached the GPS device to the defendant's property, *id.* at 949, five justices in two concurring opinions expressed concern about whether prolonged GPS monitoring of an individual's public movements implicated the Fourth Amendment, *see id.* at 955-56 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring in judgment).[20]

This Court should decline Plaintiffs' invitation to place reliance on the concurrences in *Jones*. First and foremost, *Jones* did not overrule *Smith* and this Court is bound by *Smith*. *See Agostini v. Felton*, 521 U.S. 203, 237 (1997); *ACLU*, 2013 WL 6819708, at *22. Also, the concern in *Jones* that GPS monitoring could be used to generate a comprehensive record of a person's movements, reflecting information about her personal associations, 132 S. Ct. at 955-56 (Sotomayor, J., concurring), arose from the fact that law enforcement used a GPS device to track a particular individual's whereabouts for nearly a month, and used that information to prosecute him. Here, by contrast, the FISC's orders prohibit use of the metadata to create profiles of ordinary Americans and records of their associations, and there is no allegation, much less proof, that the Government has done so in Plaintiffs' case. *See* Gov't Mot. at 5-8. Accordingly, *Smith* is not distinguishable and controls here.[21]

B. Statutory Provisions Enacted Subsequent to *Smith* Do Not Create Fourth Amendment Expectations of Privacy.

Plaintiffs argue that their asserted expectation of privacy is "buttressed" by statutory provisions enacted since *Smith* that generally prohibit telecommunications carriers from disclosing records about their customers' communications to the government. *See* Pls.' Opp. at

[20] Contrary to Plaintiffs' suggestion, *see* Pls.' Opp. at 38, the Court in *Jones* expressly disclaimed reliance on the duration of the monitoring (a factor on which the court below relied) as a basis for concluding that a search had occurred. *Jones*, 132 S. Ct. at 954.

[21] Because Plaintiffs have no possessory interest or reasonable expectation of privacy in these third party business records that has been infringed upon, Count V of their Amended Complaint for the return of telephony metadata must fail. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1173 (9th Cir. 2010) ("Rule 41(g) is concerned with those whose property or privacy interests are impaired by the seizure."). But even if this were not so, Rule 41(g) of the Federal Rules of Criminal Procedure applies only when a movant seeks "to recover property seized in connection with a criminal investigation." *United States v. Garcia*, 65 F.3d 17, 21 (4th Cir. 1995); *see also Comprehensive Drug Testing, Inc.*, 621 F.3d at 1166, 1172-74; 3C Wright & Miller, Fed. Prac. & Proc. Crim. § 690 (4th ed. 2013). The metadata are collected here for purposes of counter-terrorism investigations. *See* 50 U.S.C. §§ 1861(a)(1).

34-35 (citing statutes). This is not so. Notwithstanding these statutory enactments, the Ninth Circuit and other courts continue to hold that *Smith* applies to telecommunications records such as telephony call data, *United States v. Reed*, 575 F.3d 900, 914 (9th Cir. 2009), text message addressing information, *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 905 (9th Cir. 2008), *rev'd on other grounds*, 130 S. Ct. 2619 (2010), to/from addresses of e-mail messages and website IP addresses, *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), and Internet subscriber information, *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).[22]

These rulings reflect the principle that any rights created by these communications privacy statutes do not affect the protections afforded by the Constitution. The enactment of the Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3401 *et seq.*, following the decision in *United States v. Miller*, 425 U.S. 435 (1976), is illustrative. In *Miller* the Supreme Court ruled that a bank depositor had no Fourth Amendment expectation of privacy in his bank records because he had voluntarily conveyed the information they contained to a third party. *Miller*, 425 U.S. at 442-44. (The *Smith* Court subsequently relied on this same rationale regarding telephony records, *Smith*, 442 U.S. at 744.) Congress, in response to *Miller*, enacted the RFPA to provide a "statutory right[ ]" to privacy in bank records, *United States v. Mann*, 829 F.2d 849, 851 (9th Cir. 1987), because, "while the Supreme Court found no constitutional right of privacy in financial records, it is clear Congress may provide protection of individual rights beyond that afforded in the Constitution." H.R. Rep. No. 1383, 95th Cong., 2d Sess. 33-34, *reprinted in* 1978 U.S.C.C.A.N. 9273, 9305-06. And because the "rights created by Congress are statutory, not constitutional," *United States v. Kington*, 801 F.2d 733, 737 (5th Cir. 1986); *see also Mann*, 829 F.2d at 851-53, courts continue to apply the rationale of *Miller* to find no Fourth Amendment

[22] *See also, e.g., United States v. Christie*, 624 F.3d 558, 573 (3d Cir. 2010) ("Federal courts have uniformly held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation because it is voluntarily conveyed to third parties.") (internal quotations omitted); *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (same); *Guest v. Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001) (Internet subscriber information); *United States v. Moalin*, 2013 WL 6079518, at *5, 7 (S.D. Cal. Nov. 18, 2013) (telephony metadata); In re *Application of the United States*, 830 F. Supp. 2d 114, 133-38 (E.D. Va. 2011) (Internet Protocol addresses); *United States v. Qing Li*, 2008 WL 789899, at *4-5 (S.D. Cal. Mar. 20, 2008) (IP log-in histories and addressing information).

search in the government's collection of bank records, even if a statutory violation occurred. *See, e.g., id.* The holding of *Smith* is likewise unaffected by subsequent statutory enactments.[23]

C. The NSA's Acquisition of Telephony Metadata Is Reasonable.

Even if the telephony metadata program involved a Fourth Amendment search, it would be reasonable under the special needs doctrine. *See* Gov't Mot. at 36-37. Plaintiffs argue that the special needs doctrine does not apply in light of *Al Haramain Islamic Found., Inc. v. U.S. Dep't of Treasury*, 686 F.3d 965 (9th Cir. 2011), and because the value of the program "is sharply disputed." *See* Pls.' Opp. at 38-39. Both of these arguments are meritless.

The telephony metadata program does not resemble the program at issue in *Al Haramain*. Pls.' Opp. at 38. The blocking order at issue in that case—which froze all assets of a *known* entity designated as a terrorist organization—"shut[] down" all of the entity's operations "by design." 686 F.3d at 992. The government agency issuing the order also failed to provide "any reason why it could not have obtained a warrant" in the particular situation. *Id.* at 993; *see also id.* ("The number of designated persons located within the United States appears to be very small. The warrant requirement therefore will be relevant in only a few cases.").

The telephony metadata collection program, on the other hand, collects non-content information in order to discover and identify *unknown* terrorist operatives and prevent terrorist attacks, Primary Order at 1-3; Aug. 29 FISC Op. at 4, affects individual subscribers only minimally by design, *see* Gov't Mot. at 4-8, and protects any minimal privacy interests in telephony metadata through stringent, statutorily mandated restrictions on access to, review, and dissemination of the data that are written into the FISC's orders. *Compare* Primary Order at 4-14, *and King*, 133 S. Ct. at 1979 (safeguards limiting DNA analysis to identification information alone reduced any intrusion into privacy), *with Al Haramain*, 686 F.3d at 993 (highlighting lack of any safeguards or protections afforded the blocked entities). Unlike the

[23] In support of their argument that the voluntary conveyance of calling information to telephone companies "does not destroy the reasonableness of their expectation of privacy," Pls.' Opp. at 35, Plaintiffs rely on three cases, none of which involve information voluntarily disclosed to third parties. *See Ferguson v. Charleston*, 532 U.S. 67, 75-77 & n.9, 78, 86 (2001) (nonconsensual drug tests of pregnant women at state hospital); *Stoner v. California*, 376 U.S. 483, 489-90 (1964) (pre-*Smith* case; search of hotel guest room); *Chapman v. United States*, 365 U.S. 610, 616-18 (1961) (search of rented dwelling).

case in *Al Haramain*, which involved a "very small" number of designated persons, requiring individualized suspicion to collect the telephony metadata would be impracticable. The Government's concededly compelling interests in identifying unknown terrorist operatives and preventing terrorist attacks could not be as effectively achieved if the collection were limited to metadata pertaining to persons who have already been identified as potential terrorists, because it would not permit the type of historical analysis, contact-chaining, and timely identification of terrorist contacts that the broader collection enables. *See* Aug. 29 FISC Op. at 20-22; *ACLU*, 2013 WL 6819708, at *18. Where the program might be entirely infeasible without bulk aggregation of data, it would certainly be "impracticable" to require individualized suspicion in this context. *See Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665-66 (1989).

Plaintiffs also argue that the program does not employ the "least intrusive means" of achieving its objectives, but that is not the appropriate test under a Fourth Amendment reasonableness analysis.[24] Moreover, the issue of whether the challenged program has "prevented an impending [terrorist] attack," and the opinions of individual legislators about its intelligence value, Pls.' Opp. at 39 & nn.35-36, are not proper grounds for assessing the program's efficacy in achieving the Government's purposes. *See* Gov't Mot. at 36-37. Efficacy is judged not by statistical proof, but by program method and design. *See id. Cf. Holder v. Humanitarian Law Project*, 561 U.S. 1, 130 S. Ct. 2705, 2727-28 (2010) (recognizing that the Executive Branch may rely on predictive judgments about measures needed to detect and prevent terrorist attacks and rejecting as a "dangerous requirement" the view that specific evidence and facts must be established to demonstrate the efficacy of policies designed to thwart terrorism). At bottom, Plaintiffs (and their amici) cannot transform a policy dispute into a legal issue.[25]

[24] The Government need not show that it is using the least intrusive means available to accomplish its goal. *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls*, 536 U.S. 822, 833 (2002); *United States v. Martinez-Fuerte*, 428 U.S. 543, 556 n.12 (1976) (rejecting "less-restrictive-alternative arguments"), and even if a low percentage of positive outcomes resulted among the total number of searches or seizures, that would not render a program ineffective. *See id.* at 554; *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 454 (1990).

[25] *See, e.g.*, *Sitz*, 496 U.S. at 453-54 (consideration of effectiveness of special needs program is "not meant to transfer from politically accountable officials to the courts the decision as to which among reasonable alternative law enforcement techniques should be employed to deal with a serious public danger").

IV. PLAINTIFFS HAVE NOT PLAUSIBLY ALLEGED THAT THE TELEPHONY METADATA PROGRAM VIOLATES THE FIRST AMENDMENT.

Plaintiffs' three-paragraph opposition to the motion to dismiss their First Amendment claim is most noteworthy for what they do not argue. First, Plaintiffs concede that the challenged program is not aimed or intended to deter or punish protected speech or association. *See* Pls.' Opp. at 6-7. Second, Plaintiffs concede that the alleged First Amendment harm is not direct or substantial, but rather an "[i]ndirect and unintended limitation[] on associational interests" allegedly caused by the collection of non-content telephony metadata. *See id.* at 6; *see also ACLU*, 2013 WL 6819708, at *24 ("[T]he bulk metadata collection does not burden First Amendment rights substantially."). Thus under Ninth Circuit law, the only remaining question is whether, as Plaintiffs note, the Government's conduct is "'justified by a legitimate … purpose that outweighs'" the concededly "indirect and unintended limitations on associational interests." Pls.' Opp. at 6 (quoting *United States v. Mayer*, 503 F.3d 740, 753 (9th Cir. 2007)).

The answer to this question is yes, for at least two reasons. First, as we have explained, Plaintiffs' claim that the FISC-authorized collection of telephony metadata violates their speech and associational rights perishes in the wake of their failed Fourth Amendment claim. *See* Gov't Mot. at 37-38. Plaintiffs allege—in derivative fashion—that bulk collection of telephony metadata disclosing "private associational connections," Am. Compl. ¶ 7, "without a valid, particularized warrant supported by probable cause violates the First, Fourth, and Fifth Amendments." *Id.* ¶ 10; *see also id.* ¶ 9 (same as to alleged "search"). The Supreme Court and Ninth Circuit have held, however, that when governmental investigative activities have an indirect impact on the exercise of First Amendment freedoms, those interests are safeguarded by scrupulous adherence to Fourth Amendment standards. *See, e.g.*, *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *Mayer*, 503 F.3d at 747-50. Accordingly, "surveillance consistent with Fourth Amendment protections . . . does not violate First Amendment rights, even though it may be directed at communicative or associative activities." *Gordon v. Warren Consol. Bd. of Educ.*, 706 F.2d 778, 781 n.3 (6th Cir. 1983) (collecting cases); *United States v. Gering*, 716 F.2d 615, 620 (9th Cir. 1983);[26] *Reporters Comm. for Freedom of the Press v. AT&T Co.*, 593 F.2d 1030,

[26] Plaintiffs attempt to distinguish *Gering* by arguing that it dealt "not with the freedom of association, but with . . . the free exercise clause of religion." Pls.' Opp. at 16. Plaintiffs are

1051-52 (D.C. Cir. 1978). And as the ACLU court recently found, this "consideration is built in to any section 215 application." *ACLU*, 2013 WL 6819708, at *23 (citing 50 U.S.C. § 1861) (requiring that the investigation not be conducted "solely upon the basis of activities protected by the [F]irst [A]mendment"); *see also Alliance to End Repression v. City of Chicago*, 237 F.3d 799, 802 (7th Cir. 2001) (modifying consent decree containing similar language; holding that First Amendment permits surveillance "unless the motives of the police are improper or the methods forbidden by the Fourth Amendment or other provisions of federal or state law"), *cited with approval in Mayer*, 503 F.3d at 752-53. Plaintiffs have no legitimate expectation of privacy in telephony metadata, and have failed to plausibly allege unreasonableness on the part of the program. *See* Gov't Mot. at 33-36; *ACLU*, 2013 WL 6819708, at *20-22. They cannot hide these defects behind a First Amendment claim. *Gering*, 716 F.2d at 620.

Plaintiffs' First Amendment claim also fails because, as we have previously explained, *see* Gov't Mot. at 38, the concededly compelling national security purpose of identifying terrorist operatives and preventing terrorist attacks satisfies any applicable First Amendment standard, including the "good faith" or "legitimate law enforcement interest" test referenced by Plaintiffs and set forth in *Mayer*, 503 F.3d at 752, 753. *See id.* (rejecting constitutional challenge to FBI's infiltration, recording of conversations, and collection of names and addresses of association's members for the purpose of "do[ing] research for another investigation into sex tourism," where there was "no evidence that the government undertook its investigation in order to abridge First Amendment freedoms"); *United States v. U.S. District Court (Keith)*, 407 U.S. 297, 313 (1972) (recognizing that the investigative duty and purpose of the executive branch is stronger in national security cases than "in cases of 'ordinary crime'"). For these reasons, Plaintiffs have not stated a viable First Amendment claim.

---

incorrect. The First Amendment question presented in *Gering* was whether a mail cover "violate[d] Gering's first amendment religious *and associational* rights[.]" 716 F.2d at 618 (emphasis added); *id.* at 620 ("Since Gering has failed to show that the mail covers were improperly used and burdened his free exercise or associational rights, we find no first amendment violation."); *see also United States v. Ramsey*, 431 U.S. 606, 623-24 (1977). The Ninth Circuit recognized this in *Mayer* by specifically referencing *Gering* when it concluded that the organizational plaintiffs had not plausibly alleged that the FBI's investigation "violated any protected associational or expressive rights." 503 F.3d at 748 (citing *Gering*, 716 F.2d at 620).

Rather than address these points, Plaintiffs instead take issue with arguments the Government Defendants have not made. For example, Plaintiffs assign to the Government Defendants the position that "bad faith or other ill intent [must] be pled to state a valid First Amendment claim." Pls.' Opp. at 7 (citing *Presbyterian Church*, 870 F.2d at 522).[27] The Government Defendants, however, make no such argument. Rather, as mentioned above, we have consistently argued (as is now conceded) that the program is not conducted "for the purpose of abridging first amendment freedoms" and (as also conceded) that it is designed to "further[] the compelling national interest in identifying and tracking terrorist operatives and ultimately thwarting terrorist attacks." Gov't Mot. at 38 (internal quotation marks omitted).

Plaintiffs also insist that it is irrelevant, as a First Amendment matter, whether the telephony metadata collection program constitutes a direct or indirect burden on associational activities. *See* Pls.' Opp. at 6. But this argument is yet another straw man, for as a prerequisite to the scrutiny Plaintiffs ask this Court to apply they must allege facts that plausibly demonstrate a *substantial* burden on their First Amendment rights, whether direct or indirect, and they have not done so. *See* Gov't Mot. at 38-39.[28] The very authorities cited by Plaintiffs underscore the

[27] While Plaintiffs cite *Presbyterian Church* multiple times when addressing the merits of their First Amendment claim, *see* Pls.' Opp. 7, 14, they neglect to point out that the Ninth Circuit addressed only Article III standing in that case. *See Presbyterian Church*, 870 F.2d at 521-23. The court never reached the merits of the plaintiffs' First Amendment claim.

[28] To the extent Plaintiffs assume that exacting scrutiny applies to incidental burdens on any First Amendment activity, and outside the realm of compelled disclosures, they are wrong. The cases cited in Plaintiffs' opposition brief confirm this error. *See* Pls.' Opp. at 6-7 (collecting cases). In *Buckley v. Valeo*, the Supreme Court explained that application of exacting scrutiny requires "*significant* encroachments on First Amendment rights of the sort that compelled disclosure imposes." 424 U.S. 1, 65 (1976) (emphasis added); *see also* Pls.' Opp. at 6 (citing *Acorn Inv. v. City of Seattle*, 887 F.2d 219, 225 (9th Cir. 1989) (noting that a chilling effect "may" occur when the government "forc[es] an association . . . to disclose the names of its members," requiring the government to then establish its action "furthers a substantial governmental interest," including "a relevant correlation or substantial relation between the governmental interest and the information required to be disclosed"); *Local 1814 v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 269 (2d Cir. 1981) (applying exacting scrutiny to government-compelled disclosure of names of longshoremen who made certain political contributions); *Pollard v. Roberts*, 283 F. Supp. 248, 256-57 (E.D. Ark. 1968) ("[D]isclosure of the identities of members of the group can be compelled only by showing that there is a rational connection between such disclosure and a legitimate governmental end, and that the governmental interest in the disclosure is cogent and compelling."), *and id.* at 259 (limiting relief to the records that "would reveal the names of contributors to the Party . . . and the amounts of individual contributions"). *See ACLU*, 2013 WL 6819708, at *24 ("There must be a direct and substantial or significant burden on associational rights in order for it to qualify as substantial. Mere incidental burdens on the right to associate do not violate the First Amendment.").

shortcoming of their position, as we have previously explained. *See id.* at 38-40 (collecting compelled-disclosure cases); *see also Mayer*, 503 F.3d at 748.[29] The degree of intrusion on First Amendment interests in this case, if any, is not substantial: the FISC orders authorizing the program are not targeted at Plaintiffs, based on their associational activities or otherwise; do not compel Plaintiffs or anyone else to disclose the names or addresses of Plaintiffs' members, their clients, or anyone else with whom they associate; do not allow the Government to scrutinize their contacts indiscriminately; and have no purpose other than the compelling purpose of identifying terrorist operatives and preventing terrorist attacks. Thus, the allegation that the Government's collection of non-content metadata may have an incidental effect on Plaintiffs' associational interests fails to meet the "substantial" threshold required by the Supreme Court, Ninth Circuit, and other precedents cited by Plaintiffs for the application of "exacting" scrutiny. *See* Gov't Mot. at 38-40; *ACLU*, 2013 WL 6819708, at *24; *see also Ramsey*, 431 U.S. at 623-24.[30]

As we have previously shown, none of these defects is cured by Plaintiffs' vague and subjective declarations, *see* Gov't Mot. at 40-42, and thus Plaintiffs have failed to plausibly allege a First Amendment violation.

V. THE TELEPHONY METADATA PROGRAM DOES NOT VIOLATE THE FIFTH AMENDMENT.

A. The Telephony Metadata at Issue Is Not Covered by Any Constitutional Right to "Informational Privacy" and, Alternatively, the Challenged Program Does Not Violate Any Such Constitutional Right.

Plaintiffs' Fifth Amendment claim also fails, for want of a protected liberty or privacy interest in telephony metadata, or denial by the Government of any process to which Plaintiffs even hypothetically might be due. *See id.* at 43-45. Their invocation of a right to "informational

[29] *See also, e.g.*, *Gering*, 716 F.2d at 619 n.2 (treating same compelled-disclosure cases as "not dispositive" of whether mail covers violate the First Amendment, as those cases dealt "with a form of governmentally compelled disclosure of information" unlike the gleaning of pre-existing information on the outside of envelopes). *Gering* also supports the conclusion that the untargeted collection of telephony metadata does not constitute a direct or substantial interference with First Amendment associational rights. *Cf. id.* at 620 (affirming district court's conclusion that mail cover "was a minimally-intrusive interference" of the First Amendment).

[30] As we have explained, the telephony metadata at issue in this case do not reveal Plaintiffs' names or addresses or that of anyone with whom they speak. *See* Gov't Mot. at 5-7, 38-39. Plaintiffs' opposition is completely silent on this subject.

privacy" changes nothing.[31] It would be unprecedented for this Court to declare that collection of non-content telephony metadata from telecommunications service providers violates a constitutional or statutory "right" to "informational privacy" or "interest in avoiding disclosure of personal matters." Pls.' Opp. at 40. Indeed, Plaintiffs have not identified any Supreme Court or Ninth Circuit case recognizing, much less finding a violation of, an "informational privacy" right stemming from collection of telephone numbers or their analogs, let alone a case grounding such a "right" in the Fifth Amendment, as Plaintiffs suggest.[32] To the contrary, government compulsion and/or indiscriminate *public* disclosure of far more personal and revealing information has been found not to have violated any such alleged privacy right.[33]

For example, *In re Crawford*, 194 F.3d 954, 958 (9th Cir. 1999), upon which Plaintiffs principally rely, found no constitutional violation of any such "informational privacy" interest, even though it concerned information far more revealing than that at issue here. It involved the

[31] "Supreme Court and Ninth Circuit authority demonstrates that the constitutional right of informational privacy is murky, at best." *Huling v. City of Los Banos*, 869 F. Supp. 2d 1139, 1154 (E.D. Cal. 2012). The Supreme Court has never acknowledged the existence of such a right. *See NASA v. Nelson*, 131 S. Ct. 746, 755-57 (2011). While it has recognized that certain constitutional guarantees may create "zones of privacy," *Paul v. Davis*, 424 U.S. 693, 712-13 (1976), that right is limited to certain "fundamental" personal rights that are "implicit in the concept of ordered liberty," *Whalen v. Roe*, 429 U.S. 589, 599-03 & n.23 (1977), such as those relating to "marriage, procreation, contraception, family relationships, and child rearing and education." *Paul*, 424 U.S. at 713; *Seaton v. Mayberg*, 610 F.3d 530, 538-39 (9th Cir. 2010).

[32] While Plaintiffs attempt to use *In re Crawford*, 194 F.3d 954 (9th Cir. 1999) to support a *Fifth Amendment* substantive due process right to "informational privacy," they neglect to point out that the Ninth Circuit separated its analysis of whether a constitutional right to "informational privacy" was violated, *id.* at 958-60, from whether the plaintiff's substantive due process rights were violated, *id.* at 961. Furthermore, because Plaintiffs' allegations involve the collection of telephony metadata, not any public disclosure by the Government, the Fourth Amendment is the proper basis for any claimed privacy interest. *See Nelson*, 131 S. Ct. at 756 & n.8, *and id.* at 765 (Scalia, J., concurring) ("Respondents challenge the Government's *collection* of their private information. But the Government's collection of private information is regulated by the Fourth Amendment[.]") (quoting *County of Sacramento v. Lewis*, 524 U.S. 833, 842 (1998) ("Where a particular Amendment provides an explicit textual source of constitutional protection against a particular sort of government behavior, that Amendment, not the more generalized notion of substantive due process, must be the guide for analyzing these claims.")); *Fisher v. United States*, 425 U.S. 391, 401 (1976) ("We cannot cut the Fifth Amendment completely loose from the moorings of its language, and make it serve as a general protector of privacy[—]a word not mentioned in its text and a concept directly addressed in the Fourth Amendment.").

[33] *See, e.g.*, *Whalen*, 429 U.S. at 603-04 (legal and illegal drug prescriptions); *Nelson*, 131 S. Ct. at 751 (*e.g.*, illegal drug use and related treatment or counseling); *In re Crawford*, 194 F.3d at 958 (social security numbers coupled with names and addresses).

government's "indiscriminate public disclosure" of bankruptcy petition preparers' (BPPs') social security numbers which, as relevant here, the Ninth Circuit specifically distinguished from telephone numbers. *Id.* at 960, 958.[34] While the court opined that the government's public disclosure of SSNs, "especially when accompanied by names and addresses, *may* implicate the constitutional right to informational privacy" by "enhanc[ing] the risk of identity theft," *id.* at 958-59 (emphasis added), it explained that the nature of this information was unlike "inherently sensitive or intimate information" such as "HIV status, sexual orientation, or genetic makeup." *Id.* at 960. Moreover, the court held that the statute in question was justified by a legitimate government interest in addressing fraud and unauthorized practice of law in the BPP field, which outweighed any risk of harm resulting from identity theft. *Id.* It therefore held that the government could "properly disclose [this] private information." *Id.* at 959, 960.

Furthermore, the Ninth Circuit's finding of a violation of "informational privacy" at the preliminary injunction stage in *Nelson v. NASA*, which Plaintiffs quote repeatedly, was reversed in a unanimous decision by the Supreme Court. 530 F.3d 865, 881 (2008), *rev'd and remanded*, 131 S. Ct. 746 (2011). *Nelson* involved the government's compelled collection of substantive personal information from applicants for non-sensitive, low-security government contractor jobs. *See* 131 S. Ct. at 752-54 ("broad, opened-ended questions" to applicants, their references, and former employers regarding alcohol and drug use, treatment, and counseling; financial matters; all "adverse information" about the applicant's "honesty or trustworthiness," "financial integrity," "mental or emotional stability," and "general behavior or conduct"). The Supreme

[34] *See In re Crawford*, 194 F.3d at 958 ("the indiscriminate public disclosure of SSNs, especially when accompanied by names and addresses, may implicate the constitutional right to informational privacy. . . . Unlike a telephone number or even a name, an individual's SSN serves as a unique identifier that cannot be changed and is not generally disclosed by individuals to the public.") (footnotes and citation omitted). Plaintiffs fail to mention that the Ninth Circuit in *Crawford* expressly declined to consider "whether the *mere collection* of SSNs," as opposed to their public disclosure, "invade[d] any legally-protected interest of BPPs." 194 F.3d at 957-58 (emphasis added). The Supreme Court in *Whalen*—a case upon which Plaintiffs also heavily rely—suggested a meaningful constitutional difference exists between these situations, indicating that access by the government without a concomitant public disclosure "does not automatically amount to an impermissible invasion of privacy." 429 U.S. at 600, 602. When the Supreme Court revisited *Whalen* in *NASA v. Nelson*, 131 S.Ct. 746 (2011), it repeated the point and held that the government's mere collection of information did not violate an assumed privacy interest when the information was sufficiently protected against public disclosure. *Id.* at 761-62.

Court assumed without deciding that an informational privacy right existed, but went on to hold that the type of information at issue was not protected by any such right. *Id.* at 756-57. In so holding, the Court concluded that the challenged questions were "reasonable" in nature and "further[ed] the Government's interests in managing its internal operations," *id.* at 759. The Court also emphasized that because any answers containing personal information were protected from "'unwarranted disclosure[]'" and "'undue'" public dissemination, the government's conduct "'evidenced a proper concern' for individual privacy." *Id.* at 761-62 (quoting *Whalen*, 429 U.S. at 605; *Nixon*, 433 U.S. at 458-59; citing 5 U.S.C. § 552a).

Here too, even assuming *arguendo* that a constitutional right to "informational privacy" exists, the information at issue in this case—non-content telephony metadata devoid of personally identifying information and not disclosed to the public—is far afield from the kind of "inherently sensitive or intimate information" at issue in *In re Crawford*, 194 F.3d at 960, and not the sort of information courts have deemed sufficient to warrant constitutional protection under the Fifth Amendment. Not only do telephony metadata implicate none of the fundamental rights encompassed within the constitutional right to privacy, *see Whalen*, 429 U.S. at 598-99; *Seaton*, 610 F.3d at 538-39, there is no reasonable expectation of privacy in telephony metadata or in the retention of records containing such data. *See supra* Part III. *See also Nixon*, 433 U.S. at 458-59 (conducting a Fourth Amendment analysis to determine whether assumed right to "informational privacy" was violated).[35] Because there is no constitutional right to "informational privacy" in telephony metadata, it is not necessary to consider the five-factor

[35] The remaining cases Plaintiffs cite in support of their novel position deserve little response. In *Norman–Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260 (9th Cir. 1998), the Ninth Circuit denied summary judgment to the government on a claim of informational privacy involving non-consensual blood and urine testing of employees for syphilis, sickle cell trait, and pregnancy, where the defendant failed to offer a single government purpose for the tests. *Id.* at 1269-70. In *Tucson Woman's Clinic v. Eden*, 379 F.3d 531, 538 (9th Cir. 2004), the court granted partial summary judgment on an informational privacy claim in medical information that would place "an undue burden on the right to an abortion." *See id.* at 537 (statute requiring physicians who performed abortions to, *inter alia*, submit to "unbounded" inspections of their office to collect unredacted patient records—including names, addresses, full medical histories—and to release copies of fetal ultrasounds of subsequently aborted fetuses). *See also Thorne v. City of El Segundo*, 726 F.2d 459, 468-71 (9th Cir. 1983) (finding constitutional right to privacy against government-compelled disclosure and dissemination of detailed sexual history as part of employment application). None of these claims was resolved on Fifth Amendment grounds.

balancing test set forth by the Ninth Circuit in this area. *See Doe v. Attorney Gen.*, 941 F.2d 780, 796 (9th Cir. 1991) (considering, *e.g.*, type of record requested and the information it contains, adequacy of safeguards to prevent unauthorized disclosure, potential for harm in subsequent nonconsensual disclosure), *abrogated on other grounds by Lane v. Pena*, 518 U.S. 187 (1996).

Even assuming the existence of a constitutional right to informational privacy in the data at issue here that emanates from the Fifth Amendment, the program does not violate the Fifth Amendment. The Supreme Court and Ninth Circuit, employing variations of a five-factor test, have upheld government compulsion and disclosure of information considerably more sensitive and personal than that at issue here, *see supra* nn.33-34.[36]

The section 215 telephony metadata program stands on a firm constitutional foundation, considering (1) the minimally sensitive nature of the information contained in the statutorily-authorized and FISC-approved metadata collected—*i.e.*, telephone numbers and other non-content metadata "not includ[ing] the substantive content of any communication, . . . or the name, address, or financial information of a subscriber or customer" or any party to a call (Primary Order at 3 n.1; Aug. 29 FISC Op. at 4); (2) the "reasonable, articulable suspicion" limitation on government access to the metadata (Primary Order at 6-9);[37] (3) the lack of any public disclosure of the information whatsoever,[38] (4) the minimization procedures that also restrict *internal* access to, use, dissemination, and retention of the data to valid counter-terrorism purposes (*id.* at 4-17; 50 U.S.C. § 1861(b)(2)(B), (c)(1), (g)(2), (h)); and (5) the compelling national security interest involved (*see, e.g.*, *supra*, at 18).

---

[36] Plaintiffs insist the Government must show that its collection of telephony metadata is "narrowly tailored to meet legitimate interests." Pls.' Opp. at 40 (citing *Doe*, 941 F.3d at 796) (involving FBI's compelled disclosure of individual's HIV status). But the Supreme Court rejected such a standard in *Nelson* as "directly contrary to *Whalen*." 131 S. Ct. at 760. In any event, the program is narrowly tailored for the reasons described in the text.

[37] *See, e.g.*, *Nixon*, 433 U.S. at 466 (agreeing that any "burden arising solely from review by professional and discreet archivists is not significant"); *Whalen*, 429 U.S. at 595 (permitting access to files limited to 17 Department of Health employees and 24 investigators).

[38] *See Nelson*, 131 S. Ct. at 761-62 (upholding government's collection of substantive "personal" information based on statutory and regulatory safeguards against "undue dissemination" and "unwarranted" public disclosure) (citing *Whalen*, 429 U.S. at 605; *Nixon*, 433 U.S. at 458-59).

B. Plaintiffs' Fifth Amendment Vagueness Claim is Meritless.

Plaintiffs' contention that the telephony metadata program violates the Fifth Amendment on vagueness grounds also fails for lack of a protected liberty interest. *See, e.g.*, *Williams v. Vidmar*, 367 F. Supp. 2d 1265, 1275 (N.D. Cal. 2005) ("Since no constitutionally-protected activity is being restricted, there can be no claim that the procedures used to impose the restrictions are constitutionally insufficient."). In any event, the void-for-vagueness doctrine is inapplicable here. Under that doctrine, a statute violates due process of law if it "either *forbids or requires the doing of an act* in terms so vague that [persons] of common intelligence must necessarily guess at its meaning and differ as to its application." *Roberts v. U.S. Jaycees*, 468 U.S. 609, 629 (1984) (emphasis added). Every vagueness case cited by Plaintiffs recognizes that the doctrine contemplates a statute that forbids or regulates conduct through criminal or civil penalties. *See City of Chicago v. Morales*, 527 U.S. 41, 45, 56-59 (1999); *Kolender v. Lawson*, 461 U.S. 352, 353, 357-58 (1983); *Coates v. Cincinnati*, 402 U.S. 611, 612, 616-17 (1971).

The statutory provision Plaintiffs challenge, however, does not "forbid[ ] or require[ ]" them to perform any act, *Roberts*, 468 U.S. at 629. It does not criminalize, proscribe, or regulate conduct. Instead, it explains in clear and familiar terms, the procedures *the Government* must follow to obtain business records or other tangible items for purposes of FBI counter-terrorism investigations, and the standard that the FISC must apply in evaluating the FBI's applications for such information. *See* 18 U.S.C. § 1861(a)(1), (b)(2)(A)-(B), (g), (h); Primary Order at 1-2, 4-17; Aug. 29 FISC Op. at 28. The void-for-vagueness doctrine is therefore inapplicable.

CONCLUSION

For these and the reasons stated in the Government Defendants' initial brief, Plaintiffs' First Amended Complaint should be dismissed.[39]

[39] Plaintiffs indicate in the caption of their amended complaint—but nowhere else—that they are suing the individually named defendants in their personal as well as their official capacities. As the Ninth Circuit has ruled, government officials cannot be sued in an individual capacity for equitable relief such as Plaintiffs clearly (and only) seek here. *See Wolfe v. Strankman*, 392 F.3d 358, 360 n.2 (9th Cir. 2004) ("[T]he declaratory and injunctive relief Wolfe seeks is only available in an official capacity suit."). Accordingly, dismissal of Plaintiffs' claims against the Government Defendants requires dismissal of the case in its entirety.

Dated: February 21, 2014

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
BRYAN DEARINGER
Trial Attorney
bryan.dearinger@usdoj.gov
RODNEY PATTON
Trial Attorney
rodney.patton@usdoj.gov
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470

Attorneys for the Government Defendants Sued in their Official Capacities