2013 WL 6819708
United States District Court,
S.D. New York.

AMERICAN CIVIL LIBERTIES UNION, et al.,
Plaintiffs,
v.
James R. CLAPPER, et al., Defendants.

No. 13 Civ. 3994(WHP). | Dec. 27, 2013.

Synopsis

Background: Non-profit civil rights and liberties organizations brought action seeking a declaratory judgment that the National Security Agency's (NSA) telephony metadata collection exceeded the authority granted by the Foreign Intelligence Surveillance Act (FISA) and violated the First and Fourth Amendments. Organizations moved for a permanent injunction enjoining the government from continuing the collection, and the government moved to dismiss.

Holdings: The District Court, William H. Pauley III, J., held that:

[1] government's collection of metadata related to the organizations' calls constituted an actual injury sufficient to give the organizations' standing;

[2] Administrative Procedure Act's (APA) waiver of sovereign immunity did not apply to FISA statute allowing the collection of metadata;

[3] organizations were precluded from bringing statutory cause of action challenging FISA statute allowing the collection of metadata;

[4] FISA did not preclude organizations from bringing constitutional claims;

[5] collection of virtually all telephony metadata was authorized by FISA;

[6] NSA's telephony metadata collection program did not violate the Fourth Amendment; and

[7] organizations' speculative fear that government would review metadata related to their calls was insufficient to establish a violation of First Amendment associational rights.

Plaintiffs' motion denied; defendant's motion granted.

Attorneys and Law Firms

Jameel Jaffer, Esq., Alex A. Abdo, Esq., Brett M. Kaufman, Esq., Patrick C. Toomey, Esq., Catherine N. Crump, Esq., American Civil Liberties Union, Arthur N. Eisenberg, Esq., Christopher T. Dunn, Esq., New York Civil Liberties Union, New York, NY, Laura Donohue, Esq., Georgetown Law, Bethesda, MD, for Plaintiffs.

David S. Jones, Esq., Stuart F. Delery, Esq., Marcia Berman, Esq., James J. Gilligan, Esq., Bryan Dearinger, Esq., Tara M. La Morte, Esq., Christopher B. Harwood, Esq., John D. Clopper, Esq., U.S. Attorney's Office, S.D.N.Y., New York, NY, for Defendants.

Opinion

MEMORANDUM & ORDER

WILLIAM H. PAULEY III, District Judge:

***1** The September 11th terrorist attacks revealed, in the starkest terms, just how dangerous and interconnected the world is. While Americans depended on technology for the conveniences of modernity, al-Qaeda plotted in a seventh-century milieu to use that technology against us. It was a bold jujitsu. And it succeeded because conventional intelligence gathering could not detect diffuse filaments connecting al-Qaeda.

Prior to the September 11th attacks, the National Security Agency ("NSA") intercepted seven calls made by hijacker Khalid al-Mihdhar, who was living in San Diego, California, to an al-Qaeda safe house in Yemen. The NSA intercepted those calls using overseas signals intelligence capabilities that could not capture al-Mihdhar's telephone number identifier. Without that identifier, NSA analysts concluded mistakenly that al-Mihdhar was overseas and not in the United States. Telephony metadata would have furnished the missing information and might have permitted the NSA to notify the Federal Bureau of Investigation ("FBI") of the fact that al-Mihdhar was

calling the Yemeni safe house from inside the United States.[1]

The Government learned from its mistake and adapted to confront a new enemy: a terror network capable of orchestrating attacks across the world. It launched a number of counter-measures, including a bulk telephony metadata collection program—a wide net that could find and isolate gossamer contacts among suspected terrorists in an ocean of seemingly disconnected data.

This blunt tool only works because it collects everything. Such a program, if unchecked, imperils the civil liberties of every citizen. Each time someone in the United States makes or receives a telephone call, the telecommunications provider makes a record of when, and to what telephone number the call was placed, and how long it lasted. The NSA collects that telephony metadata. If plumbed, such data can reveal a rich profile of every individual as well as a comprehensive record of people's associations with one another.

The natural tension between protecting the nation and preserving civil liberty is squarely presented by the Government's bulk telephony metadata collection program. Edward Snowden's unauthorized disclosure of Foreign Intelligence Surveillance Court ("FISC") orders has provoked a public debate and this litigation. While robust discussions are underway across the nation, in Congress, and at the White House, the question for this Court is whether the Government's bulk telephony metadata program is lawful. This Court finds it is. But the question of whether that program should be conducted is for the other two coordinate branches of Government to decide.

The American Civil Liberties Union, the American Civil Liberties Union Foundation, the New York Civil Liberties Union, and the New York Civil Liberties Foundation (collectively, "the ACLU" or Plaintiffs) bring this action challenging the legality of the NSA's telephony metadata collection program. James R. Clapper, the Director of National Intelligence; Keith B. Alexander, the Director of NSA and Chief of the Central Security Service; Charles T. Hagel, the Secretary of Defense; Eric H. Holder, the Attorney General of the United States; and James B. Comey, the Director of the FBI (collectively, "Defendants" or the "Government") are Executive Branch Department and Agency heads involved with the bulk telephony metadata collection program. The ACLU moves for a preliminary injunction and the Government moves to dismiss the complaint. For the reasons that follow, this Court grants the Government's motion to dismiss and denies the ACLU's motion for a preliminary injunction.

BACKGROUND

I. *Foreign Intelligence Surveillance Act*

***2** In 1972, the Supreme Court recognized that "criminal surveillances and those involving domestic security" are distinct, and that "Congress may wish to consider protective standards for the latter which differ from those already prescribed for [criminal surveillances]." *United States v. U.S. Dist. Court for East. Dist. of Mich. (Keith),* 407 U.S. 297, 322, 92 S.Ct. 2125, 32 L.Ed.2d 752 (1972). "Although the *Keith* opinion expressly disclaimed any ruling 'on the scope of the President's surveillance power with respect to the activities of foreign powers,' it implicitly suggested that a special framework for foreign intelligence surveillance might be constitutionally permissible." *Clapper v. Amnesty Int'l USA,* —— U.S. ——, 133 S.Ct. 1138, 1143, 185 L.Ed.2d 264 (2013) (quoting *Keith,* 407 U.S. at 322–23, 92 S.Ct. 2125) (internal citations omitted).

In 1975, Congress organized the Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities, known as the "Church Committee," to investigate and report on the Government's intelligence-gathering operations. The Church Committee concluded that the Executive Branch had engaged in widespread surveillance of U.S. citizens and that Congress needed to provide clear boundaries for foreign intelligence gathering.

In 1978, Congress did just that. Legislating against the backdrop of *Keith* and the Church Committee findings, Congress enacted the Foreign Intelligence Surveillance Act of 1978 (FISA). Pub. L. No. 95–511, 92 Stat. 1783 (codified as amended at 50 U.S.C: §§ 1801 to 1885c). FISA requires the Government to obtain warrants or court orders for certain foreign intelligence surveillance activities and created the FISC to review those applications and grant them if appropriate.

[1] While the FISC is composed of Article III judges, it operates unlike any other Article III court. Proceedings in Article III courts are public. And the public enjoys a "general right to inspect and copy public records and documents, including judicial records and documents."

Nixon v. Warner Comm'cns, Inc., 435 U.S. 589, 597–98, 98 S.Ct. 1306, 55 L.Ed.2d 570 (1978) (footnotes omitted). "The presumption of access is based on the need for federal courts, although independent—indeed, particularly because they are independent—to have a measure of accountability and for the public to have confidence in the administration of justice." *Lugosch v. Pyramid Co. of Onondaga,* 435 F.3d 110, 119 (2d Cir.2006) (quoting *United States v. Amodeo,* 71 F.3d 1044, 1048 (2d Cir.1995)); *see also Standard Chartered Bank Int'l (Americas) Ltd. v. Calvo,* 757 F.Supp.2d 258, 259–60 (S.D.N.Y.2010).[2]

But FISC proceedings are secret. Congress created a secret court that operates in a secret environment to provide judicial oversight of secret Government activities. *See* 50 U.S.C. § 1803(c) ("The record of proceedings [in the FISC] shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence."). While the notion of secret proceedings may seem antithetical to democracy, the Founding Fathers recognized the need for the Government to keep secrets. *See* U.S. Const. Art. I § 5, cl. 3. ("Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy.")

***3** Congress has long appreciated the Executive's paramount need to keep matters of national security secret. *See, e.g.,* 5 U.S.C. § 552(b)(1)(A) (first enacted July 4, 1966, Pub. L. 89–487) (The Executive is not required to disclose "matters that are specifically authorized ... by an Executive order to be kept secret in the interest of national defense" under the Freedom of Information Act). Indeed, "[s]ecrecy and dispatch" are essential ingredients to the President's effective discharge of national security. See The Federalist No. 70, at 472 (Alexander Hamilton) (J. Cooke ed., 1961). FISC is an exception to the presumption of openness and transparency—in matters of national security, the Government must be able to keep its means and methods secret from its enemies.

In 1998, Congress amended FISA to allow for orders directing common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities to provide business records to the Government. *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105–272, § 602, 112 Stat. 2396, 2410 (1998). These amendments required the Government to make a showing of "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." § 602.

After the September 11th attacks, Congress expanded the Government's authority to obtain additional records. *See* USA PATRIOT Act of 2001, Pub. L. 107–56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861) ("section 215"); Section 215 allows the Government to obtain an order "requiring the production of any tangible things (including books, records, papers, documents, and other items)," eliminating the restrictions on the types of businesses that can be served with such orders and the requirement that the target be a foreign power or their agent. The Government invoked this authority to collect virtually all call detail records or "telephony metadata." *See* infra, Part II. *See generally* David S, Kris, On the Bulk Collection of Tangible Things, 1 Lawfare Res. Pap. Ser. 4 (2013).

Bulk telephony metadata collection under FISA is subject to extensive oversight by all three branches of government. It is monitored by the Department of Justice, the intelligence Community, the FISC, and Congress. *See* Administration White Paper, *Bulk Collection of the Telephony Metadata Under Section 215 of the USA Patriot Act* 3 (Aug. 9, 2013) [hereinafter "White Paper"]. To collect bulk telephony metadata, the Executive must first seek judicial approval from the FISC. 50 U.S.C. § 1861. Then, on a semi-annual basis, it must provide reports to the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committees on the Judiciary of the House of Representatives and the Senate. 50 U.S.C. § 1871(a). Those reports must include: (1) a summary of significant legal interpretations of section 215 involving matters before the FISC; and (2) copies of all decisions, orders, or opinions of the FISC that include significant construction or interpretation of section 215. 50 U.S.C. § 1871(c).

***4** Since the initiation of the program, a number of compliance and implementation issues were discovered and self-reported by the Government to the FISC and Congress.

> In accordance with the [FISA] Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The incidents, and the Court's responses, were also

> reported to the Intelligence Committees in great detail. The Committees, the Court, and the Executive Branch have responded actively to the incidents. The Court has imposed additional safeguards. In response to compliance problems, the Director of NSA also ordered 'end-to-end' reviews of the section 215 ... programs, and created a new position, the Director of Compliance, to help ensure the integrity of future collection.

Report on the NSA's Bulk Collection Programs for USA PATRIOT Act Reauthorization (ECF No. 33–5) [hereinafter "NSA Report"]. The NSA addressed these problems. For example, in 2011, FISC Judge Bates engaged in a protracted iterative process with the Government—that included numerous written submissions, meetings between court staff and the Justice Department, and a hearing—over the Government's application for reauthorization of another FISA collection program. That led to a complete review of that program's collection and querying methods. *See generally* Mem. Op. [REDACTED], No. [REDACTED] (F.I.S.C. Oct. 3, 2011) (Bates, J.) available at http://icontherecord.tumblr.com/tagged/declassified.[3]

In August 2013, FISC Judge Eagan noted, "[t]he Court is aware that in prior years there have been incidents of non-compliance with respect to the NSA's handling of produced information. Through oversight by this Court over a period of months, those issues were resolved." *In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from* [*REDACTED*], Case No. BR 13–109, amended slip op. at 5 n. 8, 2013 WL 5741573 (F.I.S.C., Aug. 29, 2013) (released in redacted form Sept. 17, 2013). And Congress repeatedly reauthorized the statute.

In recognition of the broad intelligence gathering capability Congress granted to the Executive Branch, section 215 included a sunset provision terminating that authority at the end of 2005. But the war on terror did not end. Congress has renewed section 215 seven times.[4] In 2006, Congress amended section 215 to require the Government to provide "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109–177, § 106, 120 Stat. 192, 196 (2006) (codified as amended at 50 U.S.C. § 1861).

II. ***NSA Bulk Telephony Metadata Collection***

On June 5, 2013, *The Guardian* published a then-classified FISC "Secondary Order" directing Verizon Business Network Services to provide the NSA "on an ongoing daily basis ... all call detail records or 'telephony metadata' " for all telephone calls on its network from April 25, 2013 to July 19, 2013. *See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From Verizon Bus. Network Servs., Inc. ex. rel. MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.,* No. BR 13–80, slip op. at 24 (F.I.S.C. Apr. 25, 2013) ("*Secondary Order* "). "Telephony metadata" includes, as to each call, the telephone numbers that placed and received the call, the date, time, and duration of the call, other session-identifying information (for example, International Mobile Subscriber Identity number, International Mobile station Equipment Identity number, et cetera), trunk identifier, and any telephone calling card number. *See* Decl. of Teresa H. Shea, Director of the Signals Intelligence Directorate, NSA, dated Oct. 1, 2013, ¶ 15 (ECF No. 63); *Secondary Order* at 2. It does not include the content of any call, the name, address, or financial information of parties to the call, or any cell site location information. *See* Shea Decl. ¶ 15; *Secondary Order* at 2. In response to the unauthorized disclosure of the Secondary Order, the Government acknowledged that since May 2006, it has collected this information for substantially every telephone call in the United States, including calls between the United States and a foreign country and calls entirely within the United States. *See* Shea Decl. ¶ 13; White Paper at 3.

***5** The Secondary Order was issued pursuant to a "*Primary Order* " setting out certain "minimization" requirements for the use of telephony metadata. *See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From* [*REDACTED*], No. BR 13–80, 2013 WL 5460137 (F.I.S.C. Apr. 25, 2013) ("*Primary Order* "). The NSA stores the metadata in secure networks and access is limited to authorized personnel. *Primary Order* at 4–5. Though metadata for all telephone calls is collected, there are restrictions on how and when it may be accessed and reviewed. The NSA may access the metadata to further a terrorism investigation only by "querying" the database with a telephone number, or "identifier," that is associated with a foreign terrorist organization. Shea Decl. ¶ 19; *Primary Order* at 6–9. Before the database may be queried, a high-ranking NSA official or one of twenty specially-authorized officials

must determine there is "reasonable articulable suspicion" that the identifier is associated with an international terrorist organization that is the subject of an FBI investigation. Shea Decl. ¶¶ 20, 31; *Primary Order* at 7. The "reasonable articulable suspicion" requirement ensures an "ordered and controlled" query and prevents general data browsing. Shea Decl. ¶ 20. An identifier reasonably believed to be used by a U.S. person may not be regarded as associated with a terrorist organization solely on the basis of activities protected by the First Amendment. Shea Decl. ¶¶ 20, 31; *Primary Order* at 9. An identifier used to query telephony metadata is referred to as a "seed." Shea Decl. ¶ 20.

The results of a query include telephone numbers that have been in contact with the seed, as well as the dates, times, and durations of those calls, but not the identities of the individuals or organizations associated with responsive telephone numbers. Shea Decl. ¶ 21. The query results also include second and third-tier contacts of the seed, referred to as "hops." Shea Decl. ¶ 22. The first "hop" captures telephony metadata for the set of telephone numbers in direct contact with the seed. The second "hop" reaches telephony metadata for the set of telephone numbers in direct contact with any first "hop" telephone number. The third "hop" corrals telephony metadata for the set of telephone numbers in direct contact with any second "hop" telephone number. Shea Decl. ¶ 22. The NSA takes this information and determines "which of the results are likely to contain foreign intelligence information, related to counterterrorism, that would be of investigative value to FBI (or other intelligence agencies)." Shea Decl. ¶ 26. They provide only this digest to the FBI. Moreover, metadata containing information concerning a U.S. person may only be shared outside the NSA if an official determines "that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance." *Primary Order* at 16–17; *see also* Shea Decl. ¶¶ 28, 32.

***6** Through this sifting, "only a very small percentage of the total data collected is ever reviewed by intelligence analysts." Shea Decl. ¶ 5. In 2012, fewer than 300 identifiers were queried. Shea Decl. ¶ 24. Because each query obtains information for contact numbers up to three hops out from the seed, the total number of responsive records was "substantially larger than 300, but ... still a very small percentage of the total volume of metadata records." Shea Decl. ¶ 24. Between May 2006 and May 2009, the NSA provided the FBI and other agencies with 277 reports containing approximately 2,900 telephone numbers. Shea Decl. ¶ 26.

III. *Plaintiffs' Claims*

Plaintiffs filed this lawsuit on June 11, 2013, less than a week after the unauthorized disclosure of the Secondary Order. The ACLU, ACLU Foundation, NYCLU, and NYCLU Foundation are "non-profit organizations that engage in public education, lobbying, and pro bono litigation upholding the civil rights and liberties guaranteed by the Constitution." Compl. ¶ 24 (ECF No. 1). The ACLU and ACLU Foundation are Verizon subscribers and their telephony metadata is therefore subject to the Secondary Order. Compl. ¶¶ 28, 35. The NYCLU was a Verizon subscriber until early April 2013. Compl. ¶ 29. The NYCLU and NYCLU Foundation alleges that their metadata was collected under a previous order before the expiration of its Verizon contract. Compl. ¶ 3, 35. The ACLU and ACLU Foundation are also customers of Verizon Wireless and allege that similar orders were provided to Verizon Wireless, allowing the Government to obtain information concerning calls placed or received on the mobile telephones of ACLU employees. Compl. ¶¶ 28, 35. While the Secondary Order does not cover calls placed on Verizon Wireless's network, the Government acknowledged that it has collected metadata for substantially every telephone call in the United States since May 2006. See Shea Decl. ¶ 13; White Paper at 3.

The Plaintiffs' employees routinely communicate by telephone with each other as well as with journalists, clients, legislators, and members of the public. The Plaintiffs' assert that "their" telephone records "could readily be used to identify those who contact Plaintiffs ... and is likely to have a chilling effect." Compl. ¶ 35. The Plaintiffs' seek a declaratory judgment that the NSA's metadata collection exceeds the authority granted by section 215 and violates the First and Fourth Amendments, and it also seeks a permanent injunction enjoining the Government from continuing the collection. Compl. ¶¶ 36–38.

The Government moves to dismiss the complaint under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) for lack of standing and failure to state a claim. The ACLU moves under Rule 65 for a preliminary injunction barring the Government from "collecting [Plaintiffs'] call records" during the pendency of this action, requiring it to quarantine "all of [Plaintiffs'] call records [it] already collected," and enjoining the Government from querying metadata using any identifier associated with the

Plaintiffs. Pls. Mot. For Prelim. Inj., dated Aug. 26, 2013 at 2 (ECF No. 26) [hereinafter "Pls. Mot."].

DISCUSSION

I. *Standing*

***7** [2] [3] "[N]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies." *DaimlerChrysler Corp. v. Cuno,* 547 U.S. 332, 341, 126 S.Ct. 1854, 164 L.Ed.2d 589 (2006) (internal quotation marks and alterations omitted); *see also Rothstein v. UBS AG,* 708 F.3d 82, 89–90 (2d Cir.2013). The case-or-controversy requirement of Article III of the Constitution requires plaintiffs to establish their standing to sue. *Amnesty Int'l,* 133 S.Ct. at 1146 (citing *Raines v. Byrd,* 521 U.S. 811, 818, 117 S.Ct. 2312, 138 L.Ed.2d 849 (1997)). "The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches." *Amnesty Int'l,* 133 S.Ct. at 1146. Therefore a court's standing inquiry is "especially rigorous" when the merits of the case would require the court "to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." *Amnesty Int'l,* 133 S.Ct. at 1147 (quoting *Raines,* 521 U.S. at 819–20, 117 S.Ct. 2312).

Article III standing requires an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Monsanto Co. v. Geertson Seed Farms,* 561 U.S. 139, 130 S.Ct. 2743, 2752, 177 L.Ed.2d 461 (2010) (citing *Horne v. Flores,* 557 U.S. 433, 445, 129 S.Ct. 2579, 174 L.Ed.2d 406 (2009)). The ACLU alleges three sources of injury: (1) the Government's mere collection of the metadata related to the ACLU's telephone calls; (2) the "search" of metadata related to the ACLU's telephone calls that results when any seed is queried because the NSA must check all of the metadata it has collected to identify all telephone numbers within three hops of the seed; and (3) the chilling effect on potential ACLU clients, whistleblowers, legislators, and others who will hesitate to contact the ACLU by telephone because they know the NSA will have a record that the call occurred.

Relying on the Supreme Court's decision in *Clapper v. Amnesty International,* 133 S.Ct. 1138, the Government contends that none of these alleged injuries are "concrete, particularized, and actual or imminent." *Monsanto,* 130 S.Ct. at 2752. *Amnesty International* was a facial challenge to the FISA Amendments Act of 2008, which expanded the Government's authority, to intercept the contents of communications for foreign intelligence purposes. The *Amnesty International* plaintiffs included attorneys and human rights organizations whose work required them to communicate with individuals overseas who might be targets of Government surveillance under the FISA Amendments Act, such as Guantanamo detainees. They alleged violations under the First and Fourth Amendments. While they offered no evidence their communications had in fact been intercepted, they asserted that there was an "objectively reasonable likelihood" their communications with foreign contacts would be intercepted in the future.[5] They also argued that they suffered a present injury stemming from expensive precautions they took to avoid interception, such as traveling overseas to meet their clients in person instead of communicating electronically.

***8** The Supreme Court found the *Amnesty International* plaintiffs had suffered no injury in fact. The Court declined to assess standing based on an " 'objectively reasonable likelihood' standard," finding it "inconsistent with [the] requirement that 'threatened injury must be certainly impending to constitute injury in fact.' " *Amnesty Int'l,* 133 S.Ct. at 1147 (quoting *Whitmore v. Arkansas,* 495 U.S. 149, 158, 110 S.Ct. 1717, 109 L.Ed.2d 135 (1990)). The *Amnesty International* plaintiffs' "highly speculative fear" that their communications would be intercepted was insufficient to confer standing. *Amnesty Int'l,* 133 S.Ct. at 1148. In so holding, the Supreme Court deconstructed the *Amnesty International* plaintiffs "highly attenuated chain of possibilities":

> (1) the Government will decide to target the communications of non-U.S. persons with whom [the plaintiffs] communicate;[6]
>
> (2) in doing so, the Government will choose to invoke its authority under [the FISA Amendments Act] rather than utilizing another method of surveillance,
>
> (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy [the FISA Amendments Act's] many safeguards and are consistent with the Fourth Amendment;
>
> (4) the Government will succeed in intercepting the communications of respondents' contacts; and

(5) respondents will be parties to the particular communications that the Government intercepts.

Amnesty Int'l, 133 S.Ct. at 1148. "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending." *Amnesty Int'l,* 133 S.Ct. at 1147 (quoting *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 564 n. 2, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992)) (emphasis in original).

The *Amnesty International* plaintiffs fared no better with their second alleged injury—costly precautions taken to avoid the risk of surveillance. In the Supreme Court's view, that the plaintiffs "incurred certain costs as a reasonable reaction to a risk of harm" was insufficient "because the harm [plaintiffs sought] to avoid [was] not certainly impending." *Amnesty Int'l,* 133 S.Ct. at 1151. "Because respondents do not face a threat of certainly impending interception under [the FISA Amendments Act], the costs that they have incurred to avoid surveillance are simply the product of their fear of surveillance ... such a fear is insufficient to create standing." *Amnesty Int'l,* 133 S.Ct. at 1152 (citing *Laird v. Tatum,* 408 U.S. 1, 10–15, 92 S.Ct. 2318, 33 L.Ed.2d 154 (1972)).

Amidax Trading Group v. S.W.I.F.T. SCRL, 671 F.3d 140 (2d Cir.2011) is instructive. Amidax's bank used SWIFT[7] to transfer funds among financial institutions. After the September 11th attacks, the Office of Foreign Assets Control subpoenaed SWIFT's records to monitor the financial transactions of suspected terrorists. Amidax sued SWIFT and the Government, alleging, *inter alia,* violations of the First and Fourth Amendments. The Second Circuit held that "[t]o establish an injury in fact—and thus, a personal stake in this litigation—[Amidax] need only establish that its information was *obtained* by the government." *Amidax,* 671 F.3d at 147 (alteration in original) (emphasis added) (quoting *Amidax Trading Grp. v. S.W.I.F.T. SCRL,* 607 F.Supp.2d 500, 508 (S.D.N.Y.2009)). But because Amidax could not plausibly show the Government had collected its records, it lacked standing. *Amidax,* 671 F.3d at 148–49.

***9** [4] Here, there is no dispute the Government collected telephony metadata related to the ACLU's telephone calls. Thus, the standing requirement is satisfied. *See Amnesty Int'l,* 133 S.Ct. at 1153 (noting that the case would be different if "it were undisputed that the Government was using [the FISA Amendments Act]-authorized surveillance to acquire respondents' communications and ... the sole dispute concerned the reasonableness of respondents' preventive measures"); *see also Klayman v. Obama,* 957F.Supp.2d 1, —— – ——, 2013 WL 6571596, at *14–17 (D.D.C. Dec. 16, 2013) (finding standing for subscriber to challenge the NSA telephony metadata collection program).

The Government argues that merely acquiring an item does not implicate a privacy interest, but that is not an argument about Article III standing. Rather, it speaks to the merits of a Fourth Amendment claim. *Cf. Rakas v. Illinois,* 439 U.S. 128, 139, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978) ("Rigorous application of the principle that the rights secured by the [Fourth] Amendment are personal, in place of a notion of "standing" will produce no additional situations in which evidence must be excluded.... [T]he better analysis ... focuses on the extent of particular [individual's Fourth Amendment] rights, rather than on any theoretically separate, but invariably intertwined concept of standing.") The ACLU is not obligated at the standing stage to prove the merits of its case, only that it has "a personal stake in this litigation." *Amidax,* 671 F.3d at 147. Because the ACLU has alleged an actual injury grounded in the Government's collection of metadata related to its telephone calls, it has standing.

II. *Statutory Claim*

A. *Sovereign Immunity*

[5] [6] The United States, as sovereign, is immune from suit unless it unequivocally consents to being sued. *United States v. Mitchell,* 445 U.S. 535, 538, 100 S.Ct. 1349, 63 L.Ed.2d 607 (1980); *see also Price v. United States,* 174 U.S. 373, 375–76, 19 S.Ct. 765, 43 L.Ed. 1011 (1899) ("It is an axiom of our jurisprudence. The government is not liable to suit unless it consents thereto, and its liability in suit cannot be extended beyond the plain language of the statute authorizing it."). Section 702 of the Administrative Procedure Act ("APA") waives sovereign immunity for suits against the United States that, like this one, seek "relief other than money damages." 5 U.S.C. § 702. The APA creates a "strong presumption that Congress intends judicial review of administrative action." *Bowen v. Mich. Acad. of Family Physicians,* 476 U.S. 667, 670, 106 S.Ct. 2133, 90 L.Ed.2d 623 (1986).

[7] [8] Exceptions to the APA's broad waiver are "construed narrowly and apply only if there is 'clear and convincing evidence of legislative intention to preclude review.' " *Nat. Res. Def. Council v. Johnson,* 461 F.3d

164, 171 (2d Cir.2006) (quoting *Japan Whaling Ass'n v. Am. Cetacean Soc'y,* 478 U.S. 221, 230 n. 4, 106 S.Ct. 2860, 92 L.Ed.2d 166 (1986)). But the presumption favoring judicial review, "like all presumptions used in interpreting statutes, may be overcome by specific language or specific legislative history that is a reliable indicator of congressional intent." *Block v. Cmty. Nutrition Inst.,* 467 U.S. 340, 349, 104 S.Ct. 2450, 81 L.Ed.2d 270 (1984). In particular, "the presumption favoring judicial review of administrative action may be overcome by inferences of intent drawn from the statutory scheme as a whole." *Block,* 467 U.S. at 349, 104 S.Ct. 2450.

1. *Section 702 Exception*

***10** [9] Section 702 does not "confer[ ] 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. This carve out ensures that a plaintiff cannot "exploit[ ] the APA's waiver to evade limitations on suit contained in other statutes" because "[t]he waiver does not apply 'if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought' by the plaintiff." *Match–E–Be–Nash–She–Wish Band of Pottawatomi Indians v. Patchak,* —— U.S. ——, 132 S.Ct. 2199, 2204–05, 183 L.Ed.2d 211 (2012). Thus, " '[w]hen Congress has dealt in particularity with a claim and [has] intended a specified remedy' ... to be exclusive, that is the end of the matter; the APA does not undo the judgment." *Pottawatomi Indians,* 132 S.Ct. at 2205 (alterations in original) (quoting *Block v. North Dakota ex rel. Bd. of Univ. & Sch. Lands,* 461 U.S. 273, 286 n. 22, 103 S.Ct. 1811, 75 L.Ed.2d 840 (1983)).

The PATRIOT Act reengineered various provisions of the Wiretap Act, the Stored Communications Act, and FISA. Section 223 of the PATRIOT Act amended the Wiretap Act and the Stored Communications Act to remove the United States as a party that could be sued by an aggrieved person under those statutes. Pub. L. No. 107–56 § 223, 115 Stat. 272 (2001) (amended 18 U.S.C. § 2520(a) and 18 U.S.C. § 2707(a) to insert "other than the United States"); *Jewel v. Nat'l Sec. Agency,* —— F.Supp.2d ——, ——, 2013 WL 3829405, at *12 (N.D.Cal. July 23, 2013) (section 223 "explicitly deleted the United States from the provisions that permit an aggrieved person to sue for recovery and obtain relief, including 'preliminary and other equitable or declaratory relief [with respect to the Wiretap Act and the Stored Communications Act].' "). At the same time, section 223 created a limited right to sue the United States for money. damages for claims arising out of the Wiretap Act, the Stored Communications Act, and FISA. Specifically, part of section 223 was codified as Title 18, United States Code, Section 2712, titled "Civil actions against the United States" and is the "exclusive remedy against the United States for any claims within the purview of this section." 18 U.S.C. § 2712(d). Section 2712 allows a plaintiff to recover money damages for any "willful violation" of the Wiretap Act, the Stored Communications Act, and three provisions of FISA: (1) electronic wiretap surveillance; (2) physical searches; and (3) pen registers or trap and trace devices. 18 U.S.C. § 2712(a).

The operation of section 223—excising non-damage suits from the Wiretap Act and the Stored Communications Act and designating section 2712 as the only avenue for a civil action under the Wiretap Act, the Stored Communications Act and certain FISA sections—shows Congress's intent to permit only money damages suits under the limited circumstances delineated in section 2712. *See Jewel,* —— F.Supp.2d at ——, 2013 WL 3829405, at *12. It is unsurprising that section 2712 does not authorize monetary damage suits for section 215 violations. Congress's concern was to provide redress for privacy violations where the Government took action to generate evidence—such as electronic eavesdropping, physical searches, or the installation of pen registers or trap and trace devices[8]—but provided no statutory cause of action when evidence was created solely in the ordinary course of business of a third party.

***11** [10] This interpretation of section 215 is buttressed by FISA's overall statutory scheme: in contrast to other FISA surveillance statutes, section 215 does not authorize any action for misuse of the information obtained. *Compare* 50 U.S.C. § 1861 (use of information obtained from "tangible things" order not subject to redress under section 2712) with 50 U.S.C. § 1806(a) (use of information obtained from electronic surveillance actionable under section 2712); 50 U.S.C. § 1825(a) (same for physical searches); 50 U.S.C § 1845(a) (same for pen registers and trap and trace devices). Thus, Congress withdrew the APA's waiver of sovereign immunity for section 215. *See Pottawatomi Indians,* 132 S.Ct. at 2204–05; *see also Klayman,* 957 F.Supp.2d at —— n. 30, 2013 WL 6571596, at *12 n. 30; *Jewel,* —— F.Supp.2d at ——, 2013 WL 3829405, at *12.

2. *Section 701 Exception*

[11] Section 701 of the APA withdraws the immunity waiver "to the extent the relevant statute 'preclude[s] judicial review.' " *Block,* 467 U.S. at 345, 104 S.Ct. 2450 (alterations in original) (citing 5 U.S.C. § 701(a)(1)). "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,* 467 U.S. at 345, 104 S.Ct. 2450.

In *Block,* the Supreme Court held that a milk consumer's challenge to milk market orders issued under the Agricultural Marketing Agreement Act was precluded under APA section 701(a)(1). 467 U.S. at 347, 104 S.Ct. 2450. As the Supreme Court explained, the Agricultural Marketing Agreement Act "contemplates a cooperative venture" between the Secretary of Agriculture, milk handlers, and milk producers. *Block,* 467 U.S. at 346, 104 S.Ct. 2450. For example, the Agricultural Marketing Agreement Act provides for "agreements among the Secretary, producers, and handlers, for hearings among them, and for votes by producers and handlers." *Block,* 467 U.S. at 346–47, 104 S.Ct. 2450 (internal citations omitted). The Agricultural Marketing Agreement Act requires a handler to exhaust administrative remedies before it permitted any judicial review. *Block,* 467 U.S. at 346, 104 S.Ct. 2450. But the Agricultural Marketing Agreement Act was silent regarding milk consumers' remedies.

[12] The Supreme Court found that silence, coupled with the statutory scheme, demonstrated that milk consumers' claims were precluded. Although the Agricultural Marketing Agreement Act impacted consumer interests, the Court concluded that "the preclusion issue does not only turn on whether the interests of a particular class ... are implicated," rather, it turns on whether "Congress intended for that class to be relied upon to challenge agency disregard of the law." *Block,* 467 U.S. at 347, 104 S.Ct. 2450. The Court went on to find that "[i]n a complex scheme of this type, the omission of such a provision is sufficient reason to believe that Congress intended to foreclose consumer participation in the regulatory process." *Block,* 467 U.S. at 347, 104 S.Ct. 2450. "[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." *Block,* 467 U.S. at 349, 104 S.Ct. 2450.

***12** [13] The interplay between section 215 and FISA's statutory scheme compel the same conclusion here. Section 215 expressly provides that "[a] person receiving a production order may challenge the legality of that order by filing a petition with the pool [of FISC judges] established by section 1803(e)(1) of this title." 50 U.S.C. § 1861(f)(2)(A)(i). It also prohibits any non-FISC modification of section 215 orders: "[a]ny production or nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect." 50 U.S.C. § 1861(f)(2)(D). Like the statutory scheme in *Block,* section 215 does not provide for any person other than a recipient of an order to challenge the orders' legality or otherwise participate in the process. *See Ark. Dairy Coop. Ass'n, Inc. v. U.S. Dep't of Agr.,* 573 F.3d 815, 822 (D.C.Cir.2009) (In *Block,* "the Supreme Court did not concentrate simply on the presence or absence of an explicit right [to appeal a milk market order] but instead noted that in the 'complex scheme' of the Agricultural. Marketing Agreement Act, there was no provision for consumer participation of any kind.").

The "cooperative venture" envisioned by FISA's statutory scheme does not involve a mundane subject like milk pricing—it involves national security, a matter of vital importance. Congress's intent to keep the means and methods of the Government's intelligence gathering efforts secret from its enemies lies at the heart of FISA. Section 215 limits disclosure of orders to the narrowest group of individuals: (1) those to whom disclosure is necessary to comply with such an order; (2) an attorney to obtain legal advice on how to respond to the order; and (3) other persons as permitted by the Director of the FBI. *See* 50 U.S.C. § 1861(d).[9] Section 215 does not just exclude a target from challenging an order, it precludes their participation in any way. *See Ark. Dairy Coop. Ass'n,* 573 F.3d at 822; *Block,* 467 U.S. at 346, 104 S.Ct. 2450.

Allowing any challenge to a section 215 order by anyone other than a recipient would undermine the Government's vital interest in keeping the details of its telephone metadata collection program secret. It would also—because of the scope of the program—allow virtually any telephone subscriber to challenge a section 215 order. In *Koretoff v. Vilsack,* 614 F.3d 532, 537 (D.C.Cir.2010) the D.C. Circuit discussed such an absurdity that also cropped up in *Block.* The D.C. Circuit noted that "[a]llowing suit by consumers would mean virtually every American could challenge every agricultural marketing order.... [T]hat hard-to-fathom result was of great concern to the Supreme Court [in

Block] and informed its assessment of Congress's intent on whether such suits were precluded by the [Agricultural Marketing Agreement Act]." *Koretoff,* 614 F.3d at 537. Allowing anyone but the recipient of section 215 orders to challenge them, or to do so anywhere outside the FISC, "would severely disrupt this complex and delicate administrative scheme." *Block,* 467 U.S. at 348, 104 S.Ct. 2450. It is clear from the statutory scheme that Congress intended to preclude statutory causes of action such as this.

***13** [14] [15] Of course, this says nothing about the ACLU's constitutional claims and it is hard to image a regime where they would be barred. A constitutional claim is precluded only on a "heightened showing" demonstrating a clear intent to do so. *Webster v. Doe,* 486 U.S. 592, 603, 108 S.Ct. 2047, 100 L.Ed.2d 632 (1988). And there is no language in FISA expressly barring a constitutional claim. *See Klayman,* 957 F.Supp.2d at ——, 2013 WL 6571596, at *13.

Regarding the statutory arguments, there is another level of absurdity in this case. The ACLU would never have learned about the section 215 order authorizing collection of telephony metadata related to its telephone numbers but for the unauthorized disclosures by Edward Snowden. Congress did not intend that targets of section 215 orders would ever learn of them. And the statutory scheme also makes clear that Congress intended to preclude suits by targets even if they discovered section 215 orders implicating them. It cannot possibly be that lawbreaking conduct by a government contractor that reveals state secrets—including the means and methods of intelligence gathering—could frustrate Congress's intent. To hold otherwise would spawn mischief: recipients of orders would be subject to section 215's secrecy protocol confining challenges to the FISC, while targets could sue in any federal district court. A target's awareness of section 215 orders does not alter the Congressional calculus. The ACLU's statutory claim must therefore be dismissed.

B. ***Merits of the Statutory Claims***

[16] Even if the statutory claim were not precluded, it would fail. "A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v. NRDC,* 555 U.S. 7, 20, 129 S.Ct. 365, 172 L.Ed.2d 249 (2008) (citing *Munaf v. Geren,* 553 U.S. 674, 689–90, 128 S.Ct. 2207, 171 L.Ed.2d 1 (2008)); *see also N.Y. Progress & Prot. PAC v. Walsh,* 733 F.3d 483, 486 (2d Cir.2013). Here, the ACLU fails to demonstrate a likelihood of success on the merits of their statutory claim.

1. ***Does the Stored Communications Act Prohibit the Collection of Telephony Metadata Under Section 215?***

[17] Section 215 was enacted at the same time as an amendment to the Stored Communications Act. As amended, the Stored Communications Act prohibits communications providers from "knowingly divulg[ing]" a subscriber's records to a government entity unless one of several exceptions are met. 18 U.S.C. § 2702(a)(3). These include when the Government obtains a warrant, an administrative subpoena, a grand jury or trial subpoena, or an order issued under § 2703(d). 18 U.S.C. § 2703(c). The Government may also obtain telephony metadata with a national security letter ("NSL") issued under 18 U.S.C. § 2709.[10] An NSL does not require judicial approval. The only hurdle is a certification from the Director of the FBI or his designee that the records sought "are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. § 2709(b)(1).

***14** By contrast, section 215 allows the government an order "requiring the production of any tangible thing." Prior to its amendment, the Government's FISA authority to collect business records applied only to records from "common carrier[s], public accommodation. facilit[ies], physical storage facilit[ies], or vehicle facilit[ies]." 50 U.S.C. § 1862 (2001). Section 215 broadened the Government's authority to seek records from additional businesses. *See* 50 U.S.C § 1861 (as amended, 2008). The only limitation—relevant here—on the types of records that may be obtained with a section 215 order are that they be obtainable with a grand jury subpoena. *See* 50 U.S.C. § 1861(c)(2)(D). Section 215 contains nothing suggesting that it is limited by the Stored Communications Act. Nevertheless, Plaintiffs argue that section 215 should be interpreted narrowly to avoid any conflict with the Stored Communications Act.

[18] But this court must attempt to interpret a statute "as a symmetrical and coherent regulatory scheme, and fit, if possible, all parts into an harmonious whole" and is "guided to a degree by common sense." *Food & Drug Admin. v. Brown & Williamson Tobacco Corp.,* 529 U.S.

120, 133, 120 S.Ct. 1291, 146 L.Ed.2d 121 (2000). Read in harmony, the Stored Communications Act does not limit the Government's ability to obtain information from communications providers under section 215 because section 215 orders are functionally equivalent to grand jury subpoenas. Section 215 authorizes the Government to seek records that may be obtained with a grand jury subpoena, such as telephony metadata under the Stored Communications Act.

That conclusion is bolstered by common sense: to allow the Government to obtain telephony metadata with an NSL but not a section 215 order would lead to an absurd result. Unlike an NSL, a section 215 order requires a FISC judge to find the Government has provided a "statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant" to a foreign intelligence investigation. 50 U.S.C. § 1861(b)(2)(A). As FISC Judge Walton found,

> [i]t would have been anomalous for Congress, in enacting the USA PATRIOT Act, to have deemed *the FBI's* application of a 'relevance' standard, without prior judicial review, sufficient to obtain records subject to [the Stored Communications Act], but to have deemed *the FISC's* application of a closely similar 'relevance' standard insufficient for the same purpose. This anomaly is avoided by interpreting sections 2702–2703 as implicitly permitting the production of records pursuant to a FISC order issued under [section 215].

In re Prod. of Tangible Things from [*REDACTED*], No. BR 08–13, Supp. Op. at 5, 2008 WL 9475145 (F.I.S.C. Dec. 12, 2008) (emphasis in the original). Any dissonance between the two provisions melts away when the Stored Communications Act is read as permitting section 215 orders to obtain telephony metadata.

2. *Did Congress Ratify The Government's Interpretation of Section 215?*

***15** [19] [20] [21] "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, 129 S.Ct. 2484, 174 L.Ed.2d 168 (2009) (quoting *Lorillard v. Pons,* 434 U.S. 575, 580, 98 S.Ct. 866, 55 L.Ed.2d 40 (1978)). "When 'all (or nearly all) of the' relevant judicial decisions have given a term or concept a consistent judicial gloss, we presume Congress intended the term or concept to have that meaning when it incorporated it into a later-enacted statute." *Bruesewitz v. Wyeth LLC,* —— U.S. ——, 131 S.Ct. 1068, 1082, 1082, 179 L.Ed.2d 1 (2011) (citing *Merck & Co. v. Reynolds,* 559 U.S. 633, 130 S.Ct. 1784, 1802, 176 L.Ed.2d 582 (2010)). "The consistent gloss represents the *public* understanding of the term." *Bruesewitz,* 131 S.Ct. at 1082.

The Government argues Congress was aware of the bulk metadata collection program and ratified it by reenacting section 215. Before Congress reauthorized FISA, no judicial opinion interpreting relevance was public, which was in line with Congress's design. Congress passed FISA to engraft judicial and congressional oversight onto Executive Branch activities that are most effective when kept secret. To conduct surveillance under section 215, the Executive must first seek judicial approval from the FISC. *See* 50 U.S.C. § 1861. Then, on a semi-annual basis, it must provide reports to the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committees on the Judiciary of the House of Representatives and the Senate. 50 U.S.C. § 1871. Those Congressional reports must include: (1) a summary of significant legal interpretations of section 215 involving matters before the FISC; and (2) copies of all decisions, orders, or opinions of the FISC that include significant construction or interpretation of section 215. 50 U.S.C. § 1871.

The Congressional reports are not public and are submitted "in a manner consistent with the protection of the national security," namely, in classified, secret proceedings. 50 U.S.C. § 1871. Such Congressional proceedings are akin to application process for a section 215 order and the FISC opinions on those applications—they are all classified, secret proceedings. There is no doubt that the Congressional Committees responsible for oversight of this program knew about the FISC opinions and the Executive Branch's interpretation of section 215. But what about the rest of Congress?

In 2010 and 2011, Congress reauthorized section 215 without making any changes.[11] Prior to the 2010 reauthorization, the Executive Branch made available *to all members of Congress* a classified, five-page document

discussing the bulk telephony metadata program. On February 23, 2010, Senators Feinstein and Bond wrote to their colleagues:

> Members of the Select Committee on Intelligence have previously requested that the Executive Branch permit each Member of Congress access to information on the nature and significance of intelligence authority on which they are asked to vote. In response to these requests, the Attorney General and the Director of National Intelligence have provided a classified paper to the House and Senate Intelligence Committees on important intelligence collection made possible by authority that is subject to the approaching sunset, and asked for our assistance in making it available, in a secure setting, directly and personally to any interested Member.

***16** Letter from Sens. Feinstein & Bond to Colleagues (Feb. 23, 2010) (ECF No. 33–6). Representative Reyes addressed a similar letter to his House colleagues. See Letter from Rep. Reyes to Colleagues (Feb. 24, 2010) (ECF No. 33–7).

That classified document, which was made available prior to the vote for reauthorization and has now been declassified in part, informed the reader that "[section 215] orders generally require production of the business records ... relating to *substantially all of the telephone calls* handled by the [telecommunications] companies, including both calls made between the United States and a foreign country and calls made entirely within the United States." NSA Report.

The following year, when section 215 was again scheduled to sunset, senators were informed of an updated classified document available for their review. *See* Letter from Sens. Feinstein & Chambliss to Colleagues (Feb. 8, 2011) (ECF No. 33–11). Apparently some Senators did review it,[12] while other Members of Congress did not.[13] The House Intelligence Committee did not make the document available to members of the House. Dozens of House members elected in 2010 therefore never had an opportunity to review the classified document. While this is problematic, the Executive Branch did what it was required to do under the statutory scheme that Congress put in place to keep Congress informed about foreign intelligence surveillance.

And viewing all the circumstances presented here in the national security context, this Court finds that Congress ratified section 215 as interpreted by the Executive Branch and the FISC, when it reauthorized FISA. In cases finding ratification, it is fair to presume that Congress had knowledge of the statute's interpretation. *See Forest Grove Sch. Dist.,* 557 U.S. at 239–40, 129 S.Ct. 2484 (Congress is presumed to be aware of Supreme Court decision); *Lorillard,* 434 U.S. at 580–81, 98 S.Ct. 866 (Congress is presumed to be aware that "every court to consider the issue" has held there is a right to a jury trial in FLSA actions); *Butterbaugh v. Dep't of Justice,* 336 F.3d 1332, 1342 (Fed.Cir.2003) (congressional awareness shown by "[e]xtensive hearings, repeated efforts at legislative correction, and public controversy"); *cf. Comm'r of Internal Revenue v. Glenshaw Glass Co.,* 348 U.S. 426, 431, 75 S.Ct. 473, 99 L.Ed. 483 (1955) (declining to find ratification where there is not "the slightest affirmative indication that Congress ever had the [relevant] decision before it").

3. *Is Bulk Telephony Metadata Collection Permitted By Section 215?*

[22] To obtain a section 215 order, the Government must show (1) "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation" and (2) that the item sought must be able to be "obtained with a subpoena duces tecum ... in aid of a grand jury investigation or with any other [court] order ... directing the production of records or tangible things." 50 U.S.C. § 1861(b, c). The Government can obtain telephony metadata with grand jury subpoenas and other court orders. *See* 18 U.S.C. § 2703(c, d).

***17** **[23]** A grand jury subpoena permits the Government to obtain tangible things 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, 111 S.Ct. 722, 112 L.Ed.2d 795 (1991). The ACLU argues that the category at issue—all telephony metadata—is too broad and contains too much irrelevant information. That argument has no traction here. Because without all the data points, the Government cannot be certain it connected the

pertinent ones. As FISC Judge Eagan noted, the collection of virtually all telephony metadata is "necessary" to permit the NSA, not the FBI, to do the algorithmic data analysis that allow the NSA to determine "connections between known and unknown international terrorist operatives." *In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from* [*REDACTED*], amended slip op. at 22–23. And it was the FISC that limited the NSA's production of telephony metadata to the FBI. While section 215 contemplates that tangible items will be produced to the FBI, FISC orders require that bulk telephony metadata be produced directly—and only—to the NSA. And the FISC forbids the NSA from disseminating any of that data until after the NSA has identified particular telephony metadata of suspected terrorists. Without those minimization procedures, FISC would not issue any section 215 orders for bulk telephony metadata collection. *In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from* [*REDACTED*], amended slip op. at 23.

[24] "Relevance" has a broad legal meaning. The Federal Rules of Civil Procedure allow parties to obtain discovery "regarding any nonprivileged matter that *is relevant* to any party's claim or defense." Fed.R.Civ.P. 26(b)(1) (emphasis added). This Rule "has been construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case." *Oppenheimer Fund. Inc. v. Sanders,* 437 U.S. 340, 351, 98 S.Ct. 2380, 57 L.Ed.2d 253 (1978) (citing *Hickman v. Taylor,* 329 U.S. 495, 501, 67 S.Ct. 385, 91 L.Ed. 451 (1947)). Tangible items are "relevant" under section 215 if they bear on or could reasonably lead to other matter that could bear on the investigation.

[25] [26] Under section 215, the Government's burden is not substantial. The Government need only provide "a statement of facts showing that there are *reasonable grounds to believe* that the tangible things sought are relevant." 50 U.S.C. § 1861(b)(2)(A) (emphasis added). Because section 215 orders flow from the Government's grand jury and administrative subpoena powers, *see* 50 U.S.C. § 1861, the Government's applications are subject to deferential review. *See R. Enters., Inc.,* 498 U.S. at 301, 111 S.Ct. 722 (upholding grand jury subpoena challenged on relevancy grounds 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"); *Nat'l Labor Relations Bd. v. Am. Med. Response, Inc.,* 438 F.3d 188, 193 (2d Cir.2006) (finding that for an administrative subpoena, "the agency's appraisal of relevancy" to its investigation "must be accepted so long as it is not obviously wrong"). FISA applications for section 215 orders "are subject to 'minimal scrutiny by the courts;' both upon initial presentation and subsequent challenge." *United States v. Abu–Jihaad,* 630 F.3d 102, 130 (2d Cir.2010) (quoting *United States v. Duggan,* 743 F.2d 59, 77 (2d Cir.1984)).

***18** **[27]** The concept of relevance in the context of an investigation does not require the Government to parse out irrelevant documents at the start of its investigation. Rather, it allows that Government to get a category of materials if the category is relevant. The question of the permissible scope is generally "variable in relation to the nature, purposes and scope of the inquiry." *Okla. Press Pub. Co. v. Walling,* 327 U.S. 186, 209, 66 S.Ct. 494, 90 L.Ed. 614 (1946). Defining the reasonableness of a subpoena based on the volume of information to be produced would require the Government to determine wrongdoing before issuing a subpoena—but that determination is the primary purpose for a subpoena. *See Okla. Press Pub. Co.,* 327 U.S. at 201, 66 S.Ct. 494 (noting that administrative subpoenas are authorized "to discover and procure evidence, not to prove a pending charge or complaint, but upon which to make one"). And in the context of a counterterrorism investigation, that after-the-attack determination would be too late.

Here, there is no way for the Government to know which particle of telephony metadata will lead to useful counterterrorism information.[14] When that is the case, courts routinely authorize large-scale collections of information, even if most of it will not directly bear on the investigation. *See In re Subpoena Duces Tecum,* 228 F.3d 341, 350–51 (4th Cir.2000) (authorizing collection of 15,000 patient files); *In re Grand Jury Proceedings: Subpoenas Duces Tecum,* 827 F.2d 301 (8th Cir.1987) (authorizing collection of all wire transactions over $1,000 for a 14–month period at a particular Western Union office).

Any individual call record alone is unlikely to lead to matter that may pertain to a terrorism investigation. Approximately 300 seeds were queried in 2012 and only a "very small percentage of the total volume of metadata records" were responsive to those queries." Shea Decl. ¶ 24. But aggregated telephony metadata is relevant because it allows the querying technique to be comprehensive. And NSA's warehousing of that data

allows a query to be instantaneous. This new ability to query aggregated telephony metadata significantly increases the NSA's capability to detect the faintest patterns left behind by individuals affiliated with foreign terrorist organizations. Shea Decl. ¶¶ 46, 48. Armed with all the metadata, NSA can draw connections it might otherwise never be able to find.[15]

The collection is broad, but the scope of counterterrorism investigations is unprecedented. National security investigations are fundamentally different from criminal investigations. They are prospective—focused on preventing attacks—as opposed to the retrospective investigation of crimes. National security investigations span "long periods of time and multiple geographic regions." Decl. of Robert J. Holley, FBI Acting Assistant Director of the Counterterrorism Division, dated Oct. 1, 2013, ¶ 18 (ECF No. 62). Congress was clearly aware of the need for breadth and provided the Government with the tools to interdict terrorist threats.

***19** Relying on *In re Horowitz,* the ACLU argues that the bulk telephony metadata collection program is overbroad because section 215 orders cover large volumes of irrelevant documents. *Horowitz* involved an investigation into financial crimes spanning borders and decades—and so the scope of the grand jury subpoena was necessary broad. *In re Horowitz,* 482 F.2d 72, 79–80 (2d Cir.1973). After noting that "the failure to limit the subpoena by subject matter is not necessarily fatal," Judge Friendly narrowed the subpoena at issue to exclude categories documents that "have no conceivable relevance to any legitimate object of investigation by the federal grand jury." *Horowitz,* 482 F.2d at 79–80. He was troubled, in particular, with a subpoena that "require[d] production of all documents contained in the files, without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period." *Horowitz,* 482 F.2d at 79. The Second Circuit's exclusion of irrelevant categories of documents in *Horowitz* has no application here because telephony metadata is a category of relevant data. Any subpoena that seeks to obtain categories of documents will likely return irrelevant documents—but only that portion of a subpoena seeking an irrelevant category of documents should be quashed.

Similarly, the ACLU reliance on *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993,* 846 F.Supp. 11 (S.D.N.Y.1994) is misplaced. There, Judge Mukasey was asked to decide whether to quash a subpoena directing a party to produce computer storage devices, not categories of documents within them. Judge Mukasey recognized that a "wider grand jury investigation into obstruction and related charges indeed justifies a commensurately broader subpoena" but cannot "justify a subpoena which encompasses documents completely irrelevant to its scope, particularly because the Government has acknowledged that relevant documents can be isolated through key-word searching." *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993,* 846 F.Supp. at 13. Because the Government was unwilling to modify the subpoena, Judge Mukasey quashed it, concluding that "the subpoena at issue unnecessarily demands documents that are irrelevant to the grand jury inquiry." *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993,* 846 F.Supp. at 13–14. Like *In re Horowitz,* this reasoning is no bar here because all telephony metadata is a relevant category of information.

III. *Constitutional Claims*

[28] [29] That Congress precluded the ACLU's statutory claims does not bar its constitutional ones. "[A] complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " *Ashcroft v. Iqbal,* 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (quoting *Bell Atl. Corp. v. Twombly,* 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). To determine plausibility, courts follow a "two-pronged approach." *Iqbal,* 556 U.S. at 679, 129 S.Ct. 1937. "First, although a court must accept as true all of the allegations contained in a complaint, that tenet is inapplicable to legal conclusions, and threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Harris v. Mills,* 572 F.3d 66, 72 (2d Cir.2009) (internal punctuation omitted). Second, a court determines "whether the 'well-pleaded factual allegations,' assumed to be true, 'plausibly give rise to an entitlement to relief.' " *Hayden v. Paterson,* 594 F.3d 150, 161 (2d Cir.2010) (quoting *Iqbal,* 556 U.S. at 679, 129 S.Ct. 1937). On a motion to dismiss, courts may consider "facts stated on the face of the complaint, in the documents appended to the complaint or incorporated in the complaint by reference, and ... matters of which judicial notice may be taken." *Allen v. WestPoint–Pepperell, Inc.,* 945 F.2d 40, 44 (2d Cir.1991).

***20** For the purposes of deciding the Government's motion to dismiss, this Court does not consider the affidavits submitted in conjunction with the ACLU's motion for a preliminary injunction. *Chandler v. Coughlin,* 763 F.2d 110, 113 (2d Cir.1985) (error to

consider affidavits in support of preliminary injunction in ruling on motion to dismiss); *see also MacDonald v. Safir,* 206 F.3d 183, 191 n. 3 (2d Cir.2000).

A. *Fourth Amendment*

[30] [31] The Fourth Amendment guarantees that all people shall be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. "[T]he Fourth Amendment protects people, not places." *Katz v. United States,* 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). A "search" occurs for purposes of the Fourth Amendment when the Government violates a person's "reasonable expectation of privacy." *Katz,* 389 U.S. at 360–61, 88 S.Ct. 507 (Harlan, J., concurring); *see also United States v. Jones,* ––– U.S. ––––, 132 S.Ct. 945, 950, 181 L.Ed.2d 911 (2012); *Bond v. United States,* 529 U.S. 334, 337, 120 S.Ct. 1462, 146 L.Ed.2d 365 (2000).

[32] In *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), the Supreme Court held individuals have no "legitimate expectation of privacy" regarding the telephone numbers they dial because they knowingly give that information to telephone companies when they dial a number. 442 U.S. at 742, 99 S.Ct. 2577. *Smith* 's bedrock holding is that an individual has no legitimate expectation of privacy in information provided to third parties.[16]

Smith arose from a robbery investigation by the Baltimore police. *Smith,* 442 U.S. at 737, 99 S.Ct. 2577. Without a warrant, the police requested that the telephone company install a device known as a pen register, which recorded the numbers dialed from Smith's home. *Smith,* 442 U.S. at 737, 99 S.Ct. 2577. After Smith's arrest, he moved to suppress evidence derived from the pen register. *Smith,* 442 U.S. at 737, 99 S.Ct. 2577. Noting it had consistently "held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," *Smith,* 442 U.S. at 743–44, 99 S.Ct. 2577, the Court found that telephone customers have no subjective expectation of privacy in the numbers they dial because they convey that information to the telephone company knowing that the company has facilities to make permanent records of the numbers they dial. *Smith,* 442 U.S. at 742–43, 99 S.Ct. 2577.

[33] The privacy concerns at stake in *Smith* were far more individualized than those raised by the ACLU. *Smith* involved the investigation of a single crime and the collection of telephone call detail records collected by the telephone company at its central office, examined by the police, and related to the target of their investigation, a person identified previously by law enforcement. *See Smith,* 442 U.S. at 737, 99 S.Ct. 2577. Nevertheless, the Supreme Court found there was no legitimate privacy expectation because "[t]elephone users ... typically know that they must convey numerical information to the telephone company; that the telephone company has facilities for recording this information; and that the telephone company does in fact record this information for a variety of legitimate business purposes." *Smith,* 442 U.S. at 743, 99 S.Ct. 2577; *see also, e.g., United States v. Reed,* 575 F.3d 900, 914 (9th Cir.2009) (finding that because "data about the. 'call origination, length, and time of call' ... is nothing more than pen register and trap and trace data, there is no Fourth Amendment 'expectation of privacy.' ") (citation omitted).

***21** The ACLU argues that analysis of bulk telephony metadata allows the creation of a rich mosaic: it can "reveal a person's religion, political associations, use of a telephone-sex hotline, contemplation of suicide, addiction to gambling or drugs, experience with rape, grappling with sexuality, or support for particular political causes." Decl. of Edward Felten, Professor of Computer Science and Public Affairs, Princeton University, ¶ 42 (ECF No. 27). But that is at least three inflections from the Government's bulk telephony metadata collection. First, without additional legal justification—subject to rigorous minimization procedures—the NSA cannot even query the telephony metadata database. Second, when it makes a query, it only learns the telephony metadata of the telephone numbers within three "hops" of the "seed." Third, without resort to additional techniques, the Government does not know who any of the telephone numbers belong to. In other words, all the Government sees is that telephone number A called telephone number B. It does not know who subscribes to telephone numbers A or B. Further, the Government repudiates any notion that it conducts the type of data mining the ACLU warns about in its parade of horribles.[17]

The ACLU also argues that "[t]here are a number of ways in which the Government could perform three-hop analysis without first building its own database of every American's call records." Supp. Decl. of Edward Felten, ¶ 6 (ECF No. 68–1). That has no traction. At bottom, it is little more than an assertion that less intrusive means to collect and analyze telephony metadata could be employed. But, the Supreme Court has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment." *City of Ontario, Cal. v. Quon,* 560 U.S.

746, 130 S.Ct. 2619, 2632, 177 L.Ed.2d 216 (2010) (citing *Vernonia School Dist. 47J v. Acton,* 515 U.S. 646, 115 S.Ct. 2386, 2396, 132 L.Ed.2d 564 (1995)). That judicial-Monday-morning-quarterbacking "could raise insuperable barriers to the exercise of virtually all search-and-seizure powers" because judges engaging in after-the-fact evaluations of government conduct "can almost always imagine some alternative means by which the objectives might have been accomplished." *Quon,* 130 S.Ct. at 2632 (internal quotation marks and citations omitted).

The ACLU's pleading reveals a fundamental misapprehension about ownership of telephony metadata. In its motion for a preliminary injunction, the ACLU seeks to: (1) bar the Government from collecting "Plaintiffs' call records" under the bulk telephony metadata collection program; (2) quarantine "all of Plaintiffs' call records" already collected under the bulk telephony metadata collection program; and (3) prohibit the Government from querying metadata obtained through the bulk telephony metadata collection program using any phone number or other identifier associated with Plaintiffs. Pls. Mot. at 2.

First, the business records created by Verizon are not "Plaintiffs' call records." Those records are created and maintained by the telecommunications provider, not the ACLU. Under the Constitution, that distinction is critical because when a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information. *See Smith,* 442 U.S. at 742, 99 S.Ct. 2577. Second, the Government's subsequent querying of the telephony metadata does not implicate the Fourth Amendment—anymore than a law enforcement officer's query of the FBI's fingerprint or DNA databases to identify someone. *See Maryland v. King,* —— U.S. ——, 133 S.Ct. 1958, 1963–64, 186 L.Ed.2d 1 (2013). In the context of DNA querying, any match is of the DNA profile—and like telephony metadata additional investigative steps are required to link that DNA profile to an individual.

***22** The collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search. *Cf. United States v. Dionisio,* 410 U.S. 1, 13, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973) (Where single grand jury subpoena did not constitute unreasonable seizure, it could not be "rendered unreasonable by the fact that may others were subjected to the same compulsion"); *In re Grand Jury Proceedings: Subpoenas Duces Tecum,* 827 F.2d at 305 ("[T]he fourth amendment does not necessarily prohibit the grand jury from engaging in a 'dragnet' operation.") (citation omitted).

The ACLU's reliance on the concurring opinions in *Jones* is misplaced. In *Jones,* the police attached a GPS tracking device to the undercarriage of a vehicle without a warrant and tracked the vehicle's location for the next four weeks. 132 S.Ct. at 948. The majority held that a "search" occurred because by placing the GPS device on the vehicle, "[t]he Government physically occupied private property for the purpose of obtaining information.... [S]uch a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Jones,* 132 S.Ct. at 949 (citation omitted). In two separate concurring opinions, five justices appeared to be grappling with how the Fourth Amendment applies to technological advances. *Jones,* 132 S.Ct. at 957 (Sotomayor, J., concurring): *Jones,* 132 S.Ct. at 964 (Alito, J., concurring).

[34] But the Supreme Court did not overrule *Smith.* And the Supreme Court has instructed lower courts not to predict whether it would overrule a precedent even if its reasoning has been supplanted by later cases. "[T]he Court of Appeals should ... leav[e] to th[e Supreme] Court the prerogative of overruling its own decisions." *Agostini v. Felton,* 521 U.S. 203, 237, 117 S.Ct. 1997, 138 L.Ed.2d 391 (1997) (quoting *Rodriguez de Quijas v. Shearson/Am. Express, Inc.,* 490 U.S. 477, 484, 109 S.Ct. 1917, 104 L.Ed.2d 526 (1989)). Clear precedent applies because *Smith* held that a subscriber has no legitimate expectation of privacy in telephony metadata created by third parties. *See Smith,* 442 U.S. at 744–45, 99 S.Ct. 2577. Inferior courts are bound by that precedent.

Some ponder the ubiquity of cellular telephones and how subscribers' relationships with their telephones have evolved since *Smith.* While people may "have an entirely different relationship with telephones than they did thirty-four years ago," *Klayman,* 957 F.Supp.2d at ——, 2013 WL 6571596, at *****21, this Court observes that their relationship with their telecommunications providers has not changed and is just as frustrating. Telephones have far more versatility now than when *Smith* was decided, but this case only concerns their use as telephones. The fact that there are more calls placed does not undermine the Supreme Court's finding that a person has no subjective expectation of privacy in telephony metadata. *See Smith,* 442 U.S. at 745, 99 S.Ct. 2577. ("The fortuity of whether or not the [tele]phone company in fact elects to make a quasi-permanent record of a particular number dialed

does not ... make any constitutional difference. Regardless of the [tele]phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record.") Importantly, "what metadata is has not changed over time," and "[a]s in *Smith,* the *types* of information at issue in this case are relatively limited: [tele]phone numbers dialed, date, time, and the like." *Klayman,* 957F.Supp.2d at ——, 2013 WL 6571596, at *21 (emphasis in original). Because *Smith* controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment.

B. ***First Amendment***

***23** [35] "[I]mplicit in the right to engage in activities protected by the First Amendment [is] a corresponding right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends." *Roberts v. U.S. Jaycees,* 468 U.S. 609, 622, 104 S.Ct. 3244, 82 L.Ed.2d 462 (1984). Pervasive Government surveillance implicates not only the Fourth Amendment but also the First Amendment:

> National security cases ... often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power. History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies.

Keith, 407 U.S. at 313–14, 92 S.Ct. 2125 (internal quotation marks and citation omitted).

[36] The ACLU alleges that "[t]he fact that the government is collecting this information is likely to have a chilling effect on people who would otherwise contact Plaintiffs." Compl. ¶ 35. Significant impairments of first amendment rights "must withstand exacting scrutiny." *United States v. Alvarez,* —— U.S. ——, 132 S.Ct. 2537, 2548, 183 L.Ed.2d 574 (2012); *see also Nat'l Commodity & Barter Ass'n v. Archer,* 31 F.3d 1521, 1531 n. 4 (10th Cir.1994); *In re Grand Jury Proceedings,* 776 F.2d 1099, 1102–03 (2d Cir.1985). The Government contends, however, that "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).

The Government's argument is well-supported. *See, e.g., United States v. Mayer,* 503 F.3d 740, 747–48 (9th Cir.2007) (noting that "Fourth Amendment provides the relevant benchmark" for a challenge to a criminal investigation on First Amendment grounds); *Anderson v. Davila,* 125 F.3d 148, 160 (3d Cir.1997) ("Government's surveillance of individuals in public places does not, by itself, implicate the Constitution" absent evidence of retaliatory conduct for protected activities); *Phila. Yearly Meeting of Religious Soc. of Friends v. Tate,* 519 F.2d 1335, 1337–38 (3d Cir.1975) (upholding police surveillance activities limited to data gathering at public meetings); *United States v. Oaks,* 527 F.2d 937, 941 (9th Cir.1975) (upholding surveillance by undercover agent of public meeting of tax rebellion group); *Lustiger v. United States,* 386 F.2d 132, 139 (9th Cir.1967) (holding that "the Fourth Amendment does not preclude postal inspectors from copying information contained on the outside of sealed envelopes in the mail"); *Cohen v. United States,* 378 F.2d 751, 760 (9th Cir.1967) (rejecting First Amendment challenge to the "mail cover" practice). And this consideration is built in to any section 215 application. *See* 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").

***24** [37] [38] Here, it is unnecessary to decide whether there could be a First Amendment violation in the absence of a Fourth Amendment violation because *Amnesty International* compels the conclusion that the bulk metadata collection does not burden First Amendment rights substantially. *Cf.* 133 S.Ct. at 1152. "[D]istinguishing between incidental and substantial burdens under the First Amendment requires a different analysis, applying different legal standards, than distinguishing what is and is not routine in the Fourth Amendment ... context." *Tabbaa v. Chertoff,* 509 F.3d 89, 102 n. 4 (2d Cir.2007). There must be "a direct and substantial" or "significant" burden on associational rights in order for it to qualify as "substantial." *Tabbaa,* 509 F.3d at 101. "Mere incidental burdens on the right to

associate do not violate the First Amendment." *Tabbaa,* 509 F.3d at 101.

[39] Any alleged chilling effect here arises from the ACLU's speculative fear that the Government will review telephony metadata related to the ACLU's telephone calls. For telephony metadata to be "used to identify those who contact Plaintiffs for legal assistance or to report human-rights or civil-liberties violations," Compl. ¶ 35, it must actually be reviewed and the identities of the telephone subscribers determined. Fear that telephony metadata relating to the ACLU will be queried or reviewed or further investigated "relies on a highly attenuated chain of possibilities." *Amnesty Int'l,* 133 S.Ct. at 1148. "[S]uch a fear is insufficient to create standing," *Amnesty Int'l,* 133 S.Ct. at 1152. Neither can it establish a violation of an individual's First Amendment rights.

IV. *Remaining Preliminary Injunction Considerations*

[40] For the reasons above, the ACLU has failed to state a claim and its case must be dismissed. But even if it could show a likelihood of success on the merits, a preliminary injunction would be inappropriate. "A preliminary injunction is an 'extraordinary and drastic remedy.' It should never be awarded as of right." *Munaf,* 553 U.S. at 676, 128 S.Ct. 2207 (quoting *Yakus v. United States,* 321 U.S. 414, 440, 64 S.Ct. 660, 88 L.Ed. 834 (1944)). As discussed above, "[a], plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter,* 555 U.S. at 20, 129 S.Ct. 365.

[41] Here, the balance of the equities and the public interest tilt firmly in favor of the Government's position. "Everyone agrees that the Government's interest in combating terrorism is an urgent objective of the highest order." *Holder v. Humanitarian Law Project,* 561 U.S. 1, 130 S.Ct. 2705, 2724, 177 L.Ed.2d 355 (2010); *see also Haig v. Agee,* 453 U.S. 280, 307, 101 S.Ct. 2766, 69 L.Ed.2d 640 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.") (internal quotation marks omitted); *In re Directives* [*REDACTED*] *Pursuant to Section 105B of the Foreign Intelligence Surveillance Act,* 551 F.3d 1004, 1012 (FISA Ct.Rev.2008) ("[T]he relevant government interest—the interest in national security—is of the highest order of magnitude.").

***25** The Constitution vests the President with Executive Power. U.S. Const. Art. II. That power reaches its zenith when wielded to protect national security. *Cf. Youngstown Sheet & Tube Co. v. Sawyer,* 343 U.S. 579, 637, 72 S.Ct. 863, 96 L.Ed. 1153 (1952) (Jackson, J., concurring) ("When the President acts pursuant to an express or implied authorization from Congress," his actions are "supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion ... rest[s] heavily upon any who might attack it." (internal quotations omitted)). And courts must pay proper deference to the Executive in assessing the threats that face the nation. *Boumediene v. Bush,* 553 U.S. 723, 797, 128 S.Ct. 2229, 171 L.Ed.2d 41 (2008) ("[M]ost federal judges [do not] begin the day with briefings that may describe new and serious threats to our Nation and its people."). Any injunction dismantling the section 215 telephony metadata collection program "would cause an increased risk to national security and the safety of the American public." Shea Decl. ¶ 63. The "unique capabilities" of the telephony metadata collection program "could not be completely replicated by other means." Shea Decl. ¶ 63.

The effectiveness of bulk telephony metadata collection cannot be seriously disputed. Offering examples is a dangerous stratagem for the Government because it discloses means and methods of intelligence gathering. Such disclosures can only educate America's enemies. Nevertheless, the Government has acknowledged several successes in Congressional testimony and in declarations that are part of the record in this case. In this Court's view, they offer ample justification:

> • In September 2009, NSA discovered that an al-Qaeda-associated terrorist in Pakistan was in contact with an unknown person in the United States about efforts to perfect a recipe for explosives. NSA immediately notified the FBI, which investigated and identified the al-Qaeda contact as Colorado-based Najibullah Zazi. The NSA and FBI worked together to identify other terrorist links. The FBI executed search warrants and found bomb-making components in backpacks. Zazi confessed to conspiring to bomb the New York subway system. Through a section 215 order, NSA was able to provide a previously unknown number of one of the co-conspirators—Adis Medunjanin.
>
> • In January 2009, while monitoring an extremist in Yemen with ties to al-Qaeda, the NSA discovered a connection with Khalid Oazzani in Kansas City. NSA immediately notified the FBI, which discovered a nascent plot to attack the New York

> Stock Exchange. Using a section 215 order, NSA queried telephony metadata to identify potential connections. Three defendants were convicted of terrorism offenses.
>
> • In October 2009, while monitoring an al-Qaeda affiliated terrorist, the NSA discovered that David Headley was working on a plot to bomb a Danish newspaper office that had published cartoons depicting the Prophet Mohammed. He later confessed to personally conducting surveillance of the Danish newspaper office. He was also charged with supporting terrorism based on his involvement in the planning and reconnaissance for the 2008 hotel attack in Mumbai. Information obtained through section 215 orders was utilized in tandem with the FBI to establish Headley's foreign ties and put them in context with U.S. based planning efforts.

***26** Holley Decl. ¶ 2426; Testimony before the House Permanent Select Committee on Intelligence, dated June 18, 2013, FBI Deputy Director Sean Joyce, at 12–13 (ECF No. 33–13) [hereinafter "Joyce Testimony"].

Bulk telephony metadata collection is one tool used to thwart potential terrorist attacks. Deputy Director Joyce explained:

> Our mission is to stop terrorism, to prevent it. Not after the fact, to prevent it before it happens in the United States. And I can tell you every tool is essential and vital. And the tools as I outlined to you and their uses today have been valuable to stopping some of those plots. You ask, 'How can you put the value on an American life?' And I can tell you, its priceless.

Joyce Testimony at 52.

Of course, the considerations weighing in favor of the ACLU's position are far from trivial. The need for the telephony metadata collection program "does not make the employment by Government of electronic surveillance a welcome development—even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens." *Keith,* 407 U.S. at 312, 92 S.Ct. 2125. Just as the Constitution gives the Executive the duty to protect the nation, citizens' right to privacy is enshrined in the Bill of Rights.

Fifteen different FISC judges have found the metadata collection program lawful a total of thirty-five times since May 2006. *See* Holley Decl. ¶¶ 6, 11; *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From* [*REDACTED*], No. BR 13–158 (F.I.S.C. Oct. 11, 2013). The Government argues that "Plaintiffs are asking this Court to conclude that the FISC exceeded its authority when it authorized the NSA's bulk collection of telephony metadata, and that this Court (without the benefit of the classified applications and information available to the FISC) should substitute its judgment for the decisions that the FISC reached [35] times." Gov't Prelim. Inj. Opp. Br. at 16–17 (ECF No. 61) (internal citation omitted).

This Court is bound only by the decisions of the Second Circuit and the Supreme Court. The decisions of other district courts are often persuasive authority. The two declassified FISC decisions authorizing bulk metadata collection do not discuss several of the ACLU's arguments. They were issued on the basis of *ex parte* applications by the Government without the benefit of the excellent briefing submitted to this Court by the Government, the ACLU, and *amici curiae.*

There is no question that judges operate best in an adversarial system. "The value of a judicial proceeding ... is substantially diluted where the process is *ex parte,* because the Court does not have available the fundamental instrument for judicial judgment: an adversary proceeding in which both parties may participate." *Carroll v. President & Comm'rs of Princess Anne,* 393 U.S. 175, 183, 89 S.Ct. 347, 21 L.Ed.2d 325 (1968). At its inception, FISC judges were called on to review warrant applications, a familiar role and one well-suited for a judge to protect the rights of an individual in his absence. The FISC's role has expanded greatly since its creation in 1978.

***27** As FISA has evolved and Congress has loosened its individual suspicion requirements, the FISC has been tasked with delineating the limits of the Government's surveillance power, issuing secret decisions without the benefit of the adversarial process. Its *ex parte* procedures are necessary to retain secrecy but are not ideal for interpreting statutes. This case snows how FISC decisions may affect every American—and perhaps, their interests should have a voice in the FISC.

CONCLUSION

The right to be free from searches and seizures is

fundamental, but not absolute. As Justice Jackson famously observed: "the Bill of Rights is not a suicide-pact." *Terminiello v. City of Chicago,* 337 U.S. 1, 69 S.Ct. 894, 93 L.Ed. 1131 (1949). Whether the Fourth Amendment protects bulk telephony metadata is ultimately a question of reasonableness. *Missouri v. McNeely,* —— U.S. ——, 133 S.Ct. 1552, 1569–70, 185 L.Ed.2d 696 (2013) ("[T]he ultimate touchstone of the Fourth Amendment is reasonableness."). Every day, people voluntarily surrender personal and seemingly-private information to transnational corporations, which exploit that data for profit. Few think twice about it, even though it is far more intrusive than bulk telephony metadata collection.

There is no evidence that the Government has used any of the bulk telephony metadata it collected for any purpose other than investigating and disrupting terrorist attacks. While there have been unintentional violations of guidelines, those appear to stem from human error and the incredibly complex computer programs that support this vital tool. And once detected, those violations were self-reported and stopped. The bulk telephony metadata collection program is subject to executive and congressional oversight, as well as continual monitoring by a dedicated group of judges who serve on the Foreign Intelligence Surveillance Court.

No doubt, the bulk telephony metadata collection program vacuums up information about virtually every telephone call to, from, or within the United States. That is by design, as it allows the NSA to detect relationships so attenuated and ephemeral they would otherwise escape notice. As the September 11th attacks demonstrate, the cost of missing such a thread can be horrific. Technology allowed al-Qaeda to operate decentralized and plot international terrorist attacks remotely. The bulk telephony metadata collection program represents the Government's counter-punch: connecting fragmented and fleeting communications to re-construct and eliminate al-Qaeda's terror network.

"Liberty and security can be reconciled; and in our system they are reconciled within the framework of the law." *Boumediene,* 553 U.S. at 798, 128 S.Ct. 2229. The success of one helps protect the other. Like the 9/11 Commission observed: The choice between liberty and security is a false one, as nothing is more apt to imperil civil liberties than the success of a terrorist attack on American soil. The 9/11 Commission Report, at 395. A court's solemn duty is "to reject as false, claims in the name of civil liberty which, if granted, would paralyze or impair authority to defend [the] existence of our society, and to reject as false, claims in the name of security which would undermine our freedoms and open the way to oppression." *American Comm'cns Ass'n, C.I.O. v. Douds,* 339 U.S. 382, 445, 70 S.Ct. 674, 94 L.Ed. 925 (1950) (Jackson, J., concurring in part and dissenting in part).

***28** For all of these reasons, the NSA's bulk telephony metadata collection program is lawful. Accordingly, the Government's motion to dismiss the complaint is granted and the ACLU's motion for a preliminary injunction is denied. The Clerk of Court is directed to terminate the motions pending at ECF Nos. 25 and 32 and to mark this case closed.

1 *See generally,* The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States [hereinafter the "9/11 Report"] (2004).

2 The Judicial Conference of the United States reaffirmed the public interest in the efficient and transparent administration of justice by acknowledging that "sealing an entire case file is a last resort." Judicial Conference of the United States, *Judicial Conference Policy on Sealed Cases* (Sept. 13, 2011), available at http://www.uscourts.gov/uscourts/News/2011/docs/JudicialConferencePolicyOnSealedCivilCas.

3 The iterative process Judge Bates describes is routine in the FISC and demonstrates the FISC does not "rubberstamp" applications for section 215 orders.

> When [the Government] prepares an application for [a section 215 order, it] first submit[s] to the [FISC] what's called a "read copy," which the court staff will review and comment on. [A]nd they will almost invariably come back with questions, concerns, problems that they see. And there is an iterative process back and forth between the Government and the [FISC] to take care of those concerns so that at the end of the day, we're confident that we're presenting something that the [FISC] will approve. That is hardly a rubber stamp. It's' rather extensive and serious judicial oversight of this process.

Testimony before the House Permanent Select Committee on Intelligence, dated Jun. 18, 2013, Robert Litt, General Counsel, Office of the Director of National Intelligence at 17–18 (ECF No. 33–13).

[4] *See* An Act to Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of that Act and the Lone Wolf Provision of the Intelligence Reform and Terrorism Provision Act of 2004 to July 1, 2006, Pub. L. No. 109–160, 119 Stat. 2957 (2005); An Act to Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of Such Act, Pub. L. No. 109–170, 120 Stat. 3 (2006); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109–177, 120 Stat. 192 (2006); Department of Defense Appropriations Act, 2010, Pub. L. No. 111–118, 123 Stat. 3409 (2009); An Act to Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, Pub. L. No. 111–141, 124 Stat. 37 (2010); FISA Sunsets Extension Act of 2011, Pub. L. No. 112–3, 125 Stat. 5 (2011); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112–14, 125 Stat. 216 (2011).

[5] A panel in the Second Circuit adopted this novel view of standing. *See Amnesty Int'l USA v. Clapper,* 638 F.3d 118, 133–34, 139 (2d Cir.2011), *overruled by* —— U.S. ——, 133 S.Ct. 1138, 185 L.Ed.2d 264 (2013). This conclusion was criticized by other Second Circuit judges. *See Amnesty Int'l USA v. Clapper,* 667 F.3d 163, 194 (2d Cir.2011) (denial of rehearing en banc) (Raggi, J. dissenting) (In finding that an "objectively reasonable likelihood" standard applied, "the panel did not explain its disregard of the Supreme Court's requirement that injury must be actual or imminently threatened"). The Supreme Court expressly rejected the Second Circuit's formulation. *See Amnesty Int'l,* 133 S.Ct. at 1146, 1151.

[6] The *Amnesty International* plaintiffs were all U.S. persons. The FISA Amendments Act permits the NSA to intercept communications of U.S. persons only if they communicate with a non-U.S. person reasonably believed to be outside the United States who is the target of the surveillance. *See Amnesty Int'l,* 133 S.Ct. at 1144, 1148.

[7] SWIFT stands for Society for Worldwide Interbank Financial Telecommunication. It provides electronic instructions on how to transfer money among thousands of financial institutions worldwide. *See Amidax,* 671 F.3d at 143.

[8] Pen register and trap and trace devices are electronic devices that, respectively, record all call detail information for telephone numbers called from or to a particular telephone line. However, they do not capture the content of the call. *See* 18 U.S.C. § 3127(3, 4).

[9] During the 2005 reauthorization of section 215, Congressman Nadler offered an amendment in the Judiciary Committee that would have permitted the recipient of an order to challenge compliance in a district court. In his remarks, Congressman Nadler stated, "[This amendment] allows the recipient of a section 215 order to challenge the order in [a district] court. This is a common-sense protection that is sorely lacking in the current law. Now the recipient, not the target—this isn't good enough, but we can't do the target.... It doesn't give the target of the order the ability to go to court. He doesn't know about it. But the recipient, if they wish, can challenge it in court." H.R. Rep. 109–174, pt 1, at 128. That amendment failed. H.R. Rep. 109–174, pt 1, at 47.

[10] An NSL is an administrative subpoena, which is one of the SCA's listed exceptions. *See* 18 U.S.C. § 2703(c)(2).

[11] An Act to Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, Pub. L. No. 111–141, 124 Stat. 37 (2010); FISA Sunsets Extension Act of 2011, Pub. L. No. 112–3, 125 Stat. 5 (2011); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112–14, 125 Stat. 216(2011).

[12] For example, Senator Wyden stated, "[M]any Members of Congress have no idea how the law is being secretly interpreted by the Executive Branch." and Senator Udall echoed that sentiment: "[W]hat most people—including many Members of Congress—believe the PATRIOT Act allows the government to do ... and what government officials privately believe the PATRIOT Act allows them to do are two different things." *See* 157 Cong. Rec. S3386 (daily ed. May 26, 2011). At the time, Senators Wyden and Udall's remarks precipitated a Freedom of Information Act lawsuit by The New York Times seeking disclosure of the classified report to Congress. That case was assigned to this Court. After briefing, argument, and an *in camera* review, this Court

concluded that disclosure of the report would "enable America's adversaries to develop means to degrade and evade the nation's foreign intelligence collection capabilities" and that it would "reveal and potentially compromise intelligence sources and methods." *N.Y. Times Co. v. U.S. Dep't of Justice,* 872 F.Supp.2d 309, 316–17 (S.D.N.Y.2012).

13 Congressman Sensenbrenner asserts in an *amicus* brief that "he was not aware of the full scope of the [telephony metadata collection] program when he voted to reauthorize section 215" and that "had he been fully informed he would not have voted to reauthorize section 215 without change." Br. of *Amicus Curiae,* F. James Sensenbrenner ("*Amicus* Br.")at 9–10 (ECF No. 56). This is a curious statement: Congressman Sensenbrenner not only had access to the five-page report made available to all Congressmen, but he also, as "a long-serving member of the House Judiciary Committee", *Amicus* Br. at 1, was briefed semi-annually by the Executive Branch that included "a summary of significant legal interpretations of section 215 involving matters before the FISC" and "copies of all decisions, orders, or opinions of the FISC that include significant construction or interpretation of section 215." 50 U.S.C. § 1871.

14 There is no question that "individuals associated with international terrorist organizations use telephonic systems to communicate with one another around the world, including the United States." *In re Application,* amended slip op. at 21. And the Government " '[a]nalysts know that the terrorists' communications are located somewhere' in the metadata [database], but cannot know where until the data is aggregated and then [queried.]" *In re Application,* amended slip op. at 21.

15 Prior to September 11th, NSA did not have that capability. General Alexander summed it up aptly, "We couldn't connect the dots because we didn't have the dots." Testimony before the House Permanent Select Committee on Intelligence, dated Jun. 18, 2013, General Keith Alexander, Director of the NSA, at 61 (ECF No. 33–13) [hereinafter "Alexander Testimony"].

16 Here are just a few matters in which an individual has no constitutionally protected expectation of privacy. *See, e.g., United States v. Miller,* 425 U.S. 435, 441–43, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) (bank records); *Couch v. United States,* 409 U.S. 322, 335–36, 93 S.Ct. 611, 34 L.Ed.2d 548 (1973) (records given to accountant); *Hoffa v. United States,* 385 U.S. 293, 302–03, 87 S.Ct. 408, 17 L.Ed.2d 374 (1966) (information revealed to a confidant); *On Lee v. United States,* 343 U.S. 747, 751–53, 72 S.Ct. 967, 96 L.Ed. 1270 (1952) (information revealed to a false friend); *see also United States v.Todisco,* 667 F.2d 255, 258 (2d Cir.1981) (telephone numbers collected by a pen register). And some more recent iterations. *See, e.g., United States v. Perrine,* 518 F.3d 1196, 1204–05 (10th Cir.2008) (subscriber information provided to an internet service provider); *United States v. Lifshitz,* 369 F.3d 173, 190 (2d Cir.2004) (information from a home computer that is transmitted over the Internet or by email); *see also United States v. Meregildo,* 883 F.Supp.2d 523, 526 (S.D.N.Y.2012) (information provided to Facebook "friend"). For an excellent discussion on the third party doctrine, *see generally,* Orin S. Kerr, The Case for the Third Party Doctrine, 107 Mich. L.Rev. 561 (2009).

17 General Alexander's testimony on this point is crystal clear:

> [I]n the open press there's this discussion about pattern analysis—[that the Government is] out there doing pattern analysis on this. That is absolutely incorrect. We are not authorized to go into the data, nor are we data mining, or doing anything with the data other than those queries that we discuss, period. We're not authorized to do it. We aren't doing it. There are no automated processes running in the background pulling together data trying to figure out networks.... The only time you can do pattern analysis is, once you start the query on that query and where you go forward.

Alexander Testimony at 66.