14-42

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 14-42

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

Plaintiffs-Appellants,

(*caption continued on inside cover*)

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF FOR DEFENDANTS-APPELLEES

STUART F. DELERY
Assistant Attorney General
DOUGLAS N. LETTER
H. THOMAS BYRON III
HENRY C. WHITAKER
Attorneys
Civil Division, Appellate Staff
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
(202) 514-3180

PREET BHARARA,
United States Attorney for the Southern District of New York
DAVID S. JONES
JOHN D. CLOPPER
EMILY E. DAUGHTRY
Assistant United States Attorneys
86 Chambers Street, 3rd Floor
New York, New York 10007
(212) 637-2739

Attorneys for Defendants-Appellees

—v.—

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

Defendants-Appellees.

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

Cases:

PAGE

PAGE

PAGE

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 14-42

AMERICAN CIVIL LIBERTIES UNION, *et al.*,

Plaintiffs-Appellants,

—v.—

JAMES R. CLAPPER, IN HIS OFFICIAL CAPACITY AS DIRECTOR OF NATIONAL INTELLIGENCE, *et al.*,[1]

Defendants-Appellees.

BRIEF FOR DEFENDANTS-APPELLEES

Jurisdictional Statement

Plaintiffs invoked the district court's jurisdiction under 28 U.S.C. § 1331 and 5 U.S.C. § 702. JA 19. On December 27, 2013, the district court entered final

---

[1] Official-capacity defendants-appellees Michael S. Rogers (as Director of the National Security Agency) and James B. Comey (as Director of the Federal Bureau of Investigation) have been automatically substituted for their respective predecessors, Keith B. Alexander and Robert S. Mueller, III. *See* Fed. R. App. P. 43(c)(2).

judgment for the government, dismissing the complaint and denying plaintiffs' motion for a preliminary injunction. SPA 53, 55. Plaintiffs filed a notice of appeal on January 2, 2014. JA 393-94. This Court has jurisdiction under 28 U.S.C. § 1291.

Statement of the Issues Presented for Review

Sixteen different judges of the Foreign Intelligence Surveillance Court ("FISC") on 37 separate occasions have concluded that it is lawful for the government to obtain telecommunications companies' business records that consist of telephony metadata reflecting the time, duration, dialing and receiving numbers, and other information about telephone calls, but that do not identify the individuals involved in, or include the content of, the calls. The FISC has required the production of such business records under Section 215 of the USA PATRIOT Act, 50 U.S.C. § 1861. The issues presented are:

1. Whether plaintiffs have established their standing to challenge the Section 215 bulk telephony-metadata program.

2. Whether plaintiffs' statutory claims are precluded by the comprehensive scheme of judicial review established by the Foreign Intelligence Surveillance Act.

3. Whether the program is authorized by Section 215, 50 U.S.C. § 1861.

4. Whether the Section 215 program is consistent with the First and Fourth Amendments.

5. Whether the district court correctly denied a preliminary injunction.

Statement of the Case

A. Procedural Background

Plaintiffs, the American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, and New York Civil Liberties Foundation, brought this action against the federal government, seeking declaratory and injunctive relief based on their claims that an anti-terrorism program undertaken pursuant to court order violates the Constitution and federal statutes. The government moved to dismiss, and plaintiffs moved for a preliminary injunction. The district court, Judge William H. Pauley III, granted the motion to dismiss, and denied plaintiffs' request for a preliminary injunction. The decision below is reported at 959 F. Supp. 2d 724.

B. Factual Background

One facet of the government's intelligence-gathering capabilities aimed at combating international terrorism is a bulk telephony-metadata program that operates under the authority of a statutory provision referred to as "Section 215," which is Section 501 of the Foreign Intelligence Surveillance Act ("FISA"), as that provision was amended by Section 215 of the USA PATRIOT Act, codified at 50 U.S.C. § 1861.

1. Section 215

Congress enacted FISA in 1978 to authorize and regulate certain governmental surveillance of communications and other activities conducted to gather foreign intelligence. FISA created a special court, the FISC, composed of federal district court judges designated by the Chief Justice, to adjudicate government applications for *ex parte* orders authorized by the statute. *See id.* § 1803(a).

Section 215 authorizes the government to apply to the FISC "for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." *Id.* § 1861(a)(1). As amended in 2006, Section 215 requires that the application include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." *Id.* § 1861(b)(2)(A). Section 215 also includes other requirements to obtain an order to produce business records or other tangible things. *See*, *e.g.*, *id.* §§ 1861(a)(2)(A), (b)(2)(A) (investigation must be authorized and conducted under guidelines approved by the Attorney General under Executive Order No. 12,333 or a successor thereto); *id.* § 1861(b)(2)(B) (application must "enumerat[e] . . . minimization procedures adopted by the Attorney General . . . that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available" under

the order). If the government makes the requisite factual showing, a FISC judge "shall enter an ex parte order as requested, or as modified, approving the release of tangible things." *Id.* § 1861(c)(1).

Section 215 establishes a detailed mechanism for the recipient of such an order to challenge it in court. *See id.* § 1861(f)(2). FISA also establishes a specific process for further review of orders issued by an individual FISC judge. *See id.* §§ 1803(b), 1822(d), 1881a(h)(6); s*ee also id.* § 1803(a)(2)(A) (authorizing the FISC to sit *en banc* to review any order). Any resulting decision of the FISC is, in turn, reviewable in the FISA Court of Review and, ultimately, in the Supreme Court. *See id.* § 1861(f)(3).

Unless a Section 215 order has been "explicitly modified or set aside consistent with" § 1861(f), it "remain[s] in full effect." *Id.* § 1861(f)(2)(D). Consistent with the basic objectives of the statute, Section 215 expressly provides that "[a]ll petitions under this subsection shall be filed under seal," that the "record of proceedings . . . shall be maintained under [appropriate] security measures," and that "[j]udicial proceedings under this subsection shall be concluded as expeditiously as possible." *Id.* § 1861(f)(4) and (5). FISA does not provide for review of Section 215 orders at the behest of a third party.

In addition to this system of judicial review, FISA established specific procedures for congressional oversight. In particular, the Attorney General must furnish certain reports detailing activities under FISA to the House and Senate Intelligence and Judiciary Committees. *See id.* §§ 1808, 1826, 1846. FISA

also requires the Attorney General to report all requests made to the FISC under Section 215 to the House and Senate Intelligence and Judiciary Committees. *See id.* § 1862(a); *see also id.* §§ 1862(b) and (c), 1871(a)(4).

2. The Section 215 Bulk Telephony-Metadata Program

The United States operates a telephony-metadata intelligence-gathering program under Section 215 as part of its efforts to combat international terrorism. Telephony metadata are data about telephone calls, such as, for example, the date and time a call was made, what number a telephone called or received a call from, and the duration of a call. JA 122, 260, 262. Companies that provide telecommunications services create and maintain records of telephony metadata for their business purposes, and they provide those business records to the federal government in bulk pursuant to court orders from the FISC issued under Section 215. The data obtained under those FISC orders do not include information about the identities of individuals; the content of the calls; or the name, address, financial information, or cell site locational information of any telephone subscribers. JA 260, 263.

Under the program, the government consolidates the metadata provided by the companies into a database that includes a historical repository of metadata aggregated from certain telecommunications companies. The FISC has explained, however, that "production of all call detail records of all persons in the United States has never occurred under this pro-

gram." *See*, *e.g.*, *In re Application of Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Dkt. No. BR 13-109 (FISC Aug. 29, 2013) ("8/29/13 FISC Order"), at 4 n.5.[2] Various details of the program remain classified, precluding further explanation here of its scope, but the absence of those details cannot justify unsupported assumptions. For example, the record does not support the conclusion that the program collects "virtually all telephony metadata" about telephone calls made or received in the United States. SPA 32, quoted in Pl. Br. 12; *see also*, *e.g.*, Pl. Br. 1-2, 23, 24, 25, 48, 58. Nor is that conclusion correct. *See* Supp. Decl. of Teresa H. Shea ¶ 7, *First Unitarian Church of Los Angeles* v. *NSA*, No. 4:13cv3287 (filed Feb. 21, 2014).[3]

The government uses the telephony-metadata program as a tool to facilitate counter-terrorism investigations—specifically, to ascertain whether international terrorist organizations are communicating with operatives in the United States. When a selector, such as a telephone number, is reasonably suspected of being associated with a terrorist organization, government analysts may then, through query-

---

[2] The order is available at: http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

[3] The precise scope of the program is immaterial, however, because, as we explain, the government should prevail as a matter of law even if the scope of the program were as plaintiffs describe.

ing, obtain telephone numbers (or other metadata, such as a number associated with a particular telephone) that have been in contact within two steps, or "hops," of the suspected-terrorist selector. JA 265. This process enables analysts to identify, among other things, previously unknown contacts of individuals suspected of being associated with terrorist organizations.

The FISC first authorized the government to obtain business records consisting of bulk telephony metadata from telecommunications companies under the authority of Section 215 in May 2006. JA 262. The FISC's authorization of the program must be renewed every 90 days. Since May 2006, the FISC has renewed the program 37 times in court orders issued by sixteen different FISC judges. JA 262-63. Most recently, the FISC reauthorized the Section 215 telephony-metadata program on March 28, 2014, in an order that expires on June 20, 2014.[4]

Section 215 generally requires that FISC production orders under the statute direct that "minimiza-

---

[4] The Director of National Intelligence ("DNI") declassified the fact of that reauthorization on March 28, 2014. *See* http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1037-joint-statement-by-attorney-general-eric-holder-and-director-of-national-intelligence-james-clapper-on-the-declassification-of-renewal-of-collection-under-section-215-of-the-usa-patriot-act-50-u-s-c-sec-1861 ("3/28 AG-DNI Joint Statement").

tion procedures" governing the retention and dissemination of information obtained under that statute be followed. *See* 50 U.S.C. § 1861(c)(1) and (g). Consistent with that requirement, the FISC orders authorizing the program include comprehensive minimization procedures. JA 129-39, 263-66. For example, the government may query the database only for metadata that are within one or two steps of a query term (selector) for which there is reasonable, articulable suspicion—as determined by a federal judge under the most recent FISC orders—that the selector is associated with a foreign terrorist organization previously identified to the FISC as the subject of a counter-terrorism investigation. JA 264; *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR-14-01 (FISC Feb. 5, 2014), http://www.uscourts.gov/uscourts/courts/fisc/br14-01-order.pdf ("2/5/14 FISC Order").

The vast majority of the metadata is never reviewed by any person; in 2012, for example, government analysts used fewer than 300 suspected-terrorist selectors and the number of records responsive to such queries was a very small percentage of the total volume in the database. JA 265. Under this program, government analysts review telephony metadata only if it is within one or two steps of the suspected-terrorist selector. JA 264.[5] The database,

---

[5] The first step represents an immediate contact of the suspected-terrorist selector; the second step represents an immediate contact of the first-step contact. JA 265.

and thus the telephony metadata returned from a query, do not include the identities of individuals; the content of any calls; or the name, address, financial information, or cell site locational information of any telephone subscribers or parties to the call, because the database does not contain such information in the first place. JA 263.

The government does not use the results of Section 215 telephony metadata queries to compile comprehensive records or dossiers, even on suspected terrorists. JA 267. Instead, the government uses those results in conjunction with a range of analytical tools to ascertain those contacts that may be of use in identifying individuals who may be associated with certain foreign terrorist organizations because they have been in communication with certain suspected-terrorist telephone numbers or other selectors. JA 267. The FISC's Section 215 orders strictly prohibit NSA from disseminating any information concerning U.S. persons (which includes citizens and lawful permanent residents, *see* 50 U.S.C. § 1801(i)) unless a senior NSA official determines that the information is necessary to understand counter-terrorism information or assess its importance. JA 138, 267. NSA disseminates under the Section 215 program only the tiny fraction of metadata that are themselves associated with suspected-terrorist activity, or are responsive to queries using those suspected-terrorist selectors. JA 267. Subject to those constraints, the result of this analysis provides information the government may use in in counter-terrorism investigations.

The program is subject to a rigorous regime of safeguards and oversight, including technical and administrative restrictions on access to the database, internal NSA compliance audits, Department of Justice and Office of the Director of National Intelligence oversight, and reports both to the FISC and congressional intelligence committees. JA 267. For example, the FISC orders creating the program require NSA to report to the FISC the number of instances in which NSA has shared with other government agencies Section 215 telephony-metadata query results about U.S. persons. JA 141.

The substantial protections in the Section 215 program reflect longstanding minimization requirements imposed by FISC orders under Section 215 as well as two recent modifications to the program that were announced by the President in January 2014 and adopted in subsequent FISC orders. Prior to those modifications, the FISC orders establishing the program provided that one of 22 designated officials within the NSA had to determine that a proposed suspected-terrorist selector met the reasonable, articulable suspicion standard. JA 264, 268. The FISC orders also permitted the government to obtain query results that revealed information up to three steps away from the query selector. JA 265.

In January 2014, the President announced that he was "ordering a transition" that will "end" the "bulk metadata program as it currently exists." Remarks by the President on Review of Signals Intelligence, http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

The President announced two immediate modifications to the Section 215 program: limiting analyst review of telephony-metadata query results to contacts within two steps (rather than three) of the suspected-terrorist selector, and requiring an advance judicial finding by the FISC that the reasonable, articulable suspicion standard is satisfied as to each suspected-terrorist selector used in queries, except in emergency circumstances (in which case the FISC must retrospectively approve the selector). In February, the FISC granted the government's motion to implement those two changes to the program. *See* 2/5/14 FISC Order.

On March 27, 2014, the President further announced, after having considered options presented to him by the Intelligence Community and the Attorney General, that he will seek legislation to replace the Section 215 bulk telephony-metadata program. Statement by the President on the Section 215 Bulk Metadata Program, http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program ("3/27 President Statement"). The President stated that his goal was to "establish a mechanism to preserve the capabilities we need without the government holding this bulk metadata" to "give the public greater confidence that their privacy is appropriately protected, while maintaining the tools our intelligence and law enforcement agencies need to keep us safe." Instead of the government obtaining business records of telephony metadata in bulk, the President proposed that telephony metadata should remain in the hands of telecommunications companies. The President stated

that "legislation will be needed to permit the government to obtain information with the speed and in the manner that will be required to make this approach workable." Under such legislation, the government would be authorized to obtain telephony metadata from the companies pursuant to individualized orders from the FISC. The President explained that, in the meantime, the government would seek from the FISC a 90-day reauthorization of the existing Section 215 program, with the two modifications already approved by the FISC in February, and the court has since entered an order reauthorizing the program. *See* 3/28 AG-DNI Joint Statement.

C. This Lawsuit

Plaintiffs are nonprofit organizations engaged in public education, lobbying, and pro bono public-interest litigation. JA 23. In June 2013, plaintiffs brought this lawsuit to challenge the lawfulness of the government's Section 215 bulk telephony-metadata program. JA 17. The complaint alleged that the government had collected metadata from a telecommunications company of which plaintiffs are customers (or former customers). JA 18. Plaintiffs alleged that this telephony metadata could be used to identify individuals who contact plaintiffs, which could "have a chilling effect on people who would otherwise contact [p]laintiffs." JA 26. Plaintiffs alleged that the Section 215 program exceeds the government's statutory authority and violates their First and Fourth Amendment rights. JA 27. They sought a declaration that the Section 215 program is unconstitutional, a permanent injunction against its opera-

tion, and a purge of any metadata about plaintiffs' calls obtained under the Section 215 program. JA 27.

Approximately two months later, plaintiffs moved for a preliminary injunction. Plaintiffs sought to bar the government from obtaining, under the Section 215 program, bulk metadata about plaintiffs' calls; to require the government to quarantine any records of their calls obtained under the program; and to prohibit the government from querying the telephony metadata with any selector associated with them. JA 34. The same day, the government moved to dismiss the complaint for lack of jurisdiction and failure to state a claim. JA 118. The district court denied plaintiffs' motion for a preliminary injunction and granted the government's motion to dismiss. SPA 53.

The district court concluded, as a threshold matter, that plaintiffs had established standing to pursue their claims. Noting the absence of a dispute over whether the government had obtained metadata about plaintiffs' calls under Section 215, the court held that the mere fact that the government had obtained such records demonstrated "an actual injury grounded in the Government's collection of metadata related to [plaintiffs'] telephone calls." SPA 18.

Regarding plaintiffs' statutory claims, the district court held that it lacked jurisdiction to entertain such claims under the Administrative Procedure Act ("APA") because FISA's comprehensive scheme of judicial review precludes APA review. SPA 22-24. The court also rejected plaintiffs' statutory claims on the merits. The court observed that Congress had ratified the Section 215 bulk telephony-metadata program

through its reauthorization of the statute in 2010 and again in 2011. SPA 28-32. The court, moreover, did not agree with plaintiffs that the Stored Communications Act, 18 U.S.C. § 2702, which generally prohibits telecommunications companies from disclosing call subscriber information, prohibits the production of business records consisting of telephony metadata under Section 215, observing that Section 215 "contains nothing suggesting that it is limited by the Stored Communications Act." SPA 27.

The district court also held that the telephony-metadata program satisfies the statutory requirements in Section 215 that there be "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation," and that the item sought be obtainable by a grand jury subpoena or other court order, 50 U.S.C. § 1861(b), (c)(2)(D). SPA 32. The court pointed to the broad legal meaning of relevance in this context, and ruled that the bulk telephony metadata is indeed relevant to counter-terrorism investigations because "it allows the querying technique to be comprehensive" and permits the government to "draw connections it might otherwise never be able to find." SPA 35. The court also relied on the fact that "[n]ational security investigations . . . are prospective—focused on preventing attacks—as opposed to the retrospective investigation of crimes." SPA 36.

The district court rejected plaintiffs' constitutional claims. SPA 37. The court concluded that the Supreme Court's decision in *Smith* v. *Maryland*, 442 U.S. 735 (1979), forecloses plaintiffs' claim that the

Section 215 telephony-metadata program violates the Fourth Amendment. SPA 39-40. *Smith* held that individuals lack a Fourth Amendment privacy interest in the telephone numbers they dial because they voluntarily provide that information to their telephone providers. 442 U.S. at 742-45. The court reasoned that neither the broader scale of the program here nor changes in technology have overridden *Smith*'s bedrock holding that "when a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information." SPA 42.

The court also rejected plaintiffs' First Amendment claim. The court found that plaintiffs have made no plausible allegation that the program burdens their First Amendment rights more than incidentally. SPA 46. The court ruled as well that any alleged "chilling effects" rest on plaintiffs' speculative fear that metadata associated with their calls could be used to identify them, a fear that the Supreme Court recently rejected as a basis for standing in *Clapper* v. *Amnesty International USA*, 133 S. Ct. 1138, 1148 (2013).

The court therefore dismissed plaintiffs' complaint. The court further held that plaintiffs would not be entitled to a preliminary injunction even if they were likely to succeed on the merits because the balance of equities tips in the government's favor given its paramount interest in combating terrorism. SPA 48.

Summary of Argument

Plaintiffs have not established standing to bring this suit. They claim that the Section 215 bulk telephony-metadata program chills their activities, and the actions of those who might want to communicate with them, because government employees can learn confidential information about plaintiffs' communications. But those injuries could arise only if metadata associated with plaintiffs' calls were actually reviewed by a person, and plaintiffs do not dispute that only a small fraction of the Section 215 telephony metadata is actually reviewed by any person. There is only a speculative possibility that metadata about plaintiffs' calls would be responsive to queries using suspected-terrorist selectors, and subjective chilling effects resting on such speculation do not support Article III standing. Although plaintiffs in their brief claim injury from the mere acquisition by the government of metadata about their calls—even if no one ever sees it—plaintiffs offer no explanation for how any of their asserted injuries could plausibly flow from the mere fact that the metadata may be in the possession of the government. *See infra* Point I.

Even if plaintiffs had established standing, their statutory claims could not be brought in district court. Congress intended such issues to be resolved solely before the FISC under FISA's comprehensive and carefully limited statutory scheme for judicial review. Congress also established a limited and exclusive damages remedy that does not provide for injunctive relief for the statutory claims plaintiffs assert here. *See infra* Point II.A.

If the Court were nonetheless to reach the merits, it should affirm the district court's dismissal of the suit. Section 215 provides that the Foreign Intelligence Surveillance Court may order the production of "tangible things" "if the government has reasonable grounds to believe" that the information is relevant to an "authorized investigation." 50 U.S.C. § 1861(a)(1), (b)(2)(A). As the FISC has repeatedly concluded, the bulk telephony-metadata program under Section 215 satisfies that standard because it allows the government to draw connections between known or suspected terrorists and other, previously unknown individuals who may be acting in concert with them. *See infra* Point II.B. Congress has ratified that interpretation of Section 215 by twice extending authorization of the statute after being fully briefed on the contours of the Section 215 bulk telephony-metadata program. *See infra* Point II.C.

Plaintiffs' Fourth Amendment claim is, as the FISC has repeatedly concluded, foreclosed by the Supreme Court's decision in *Smith* v. *Maryland*, 442 U.S. 735 (1979), which held that individuals lack a Fourth Amendment privacy interest in telephone call record information provided by callers to their telecommunications companies. Plaintiffs suggest that *Smith*'s holding does not extend to bulk telephony metadata generated using modern technology, but the third-party doctrine reaffirmed in *Smith* and other cases remains binding law, and continues to serve important functions. *See infra* Point III.A.1. The existence of a Fourth Amendment privacy interest is particularly implausible here, given that it is entirely speculative whether any government analyst has ev-

er, or ever would, review metadata about plaintiffs' calls.

Even if plaintiffs possessed some minimal privacy interest in business records consisting of telephony metadata, the production of those records to the government under Section 215 is entirely reasonable and permissible under the Fourth Amendment's special needs doctrine. The telephony-metadata program serves the paramount government interest in preventing and disrupting terrorist attacks on the United States, and does so with minimal impact on legitimate privacy concerns. *See infra* Point III.A.2.

Nor do plaintiffs state a First Amendment claim. Plaintiffs' asserted First Amendment injury would depend on government personnel actually reviewing telephony metadata associated with their telephone calls (and identifying such metadata to be related to plaintiffs specifically)—an entirely speculative prospect. The program does not single out plaintiffs or any expressive activity, and any burden on First Amendment rights is incidental to the program's mission of facilitating counter-terrorism investigations. *See infra* Point III.B.

The district court thus correctly dismissed the complaint. The court further correctly concluded that a preliminary injunction would be inappropriate here in any event. An injunction may issue only if the balance of the equities tips in plaintiffs' favor. Here, the program serves important national security interests, and courts are rightly sensitive to the risks of handcuffing the government's efforts to prevent harm to the nation. *See infra* Point IV.

Standard of Review

The Court reviews *de novo* a district court's dismissal of a complaint for lack of standing and for failure to state a claim. *Town of Babylon* v. *Federal Housing Finance Agency*, 699 F.3d 221, 227 (2d Cir. 2012). To survive a motion to dismiss, 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 (2009) (internal quotation marks omitted). Mere "'labels and conclusions,'" and "'naked assertion[s]' devoid of 'further factual enhancement,'" are not sufficient. *Id.* (quoting *Bell Atlantic Corp.* v. *Twombly*, 550 U.S. 544, 555, 557 (2007)).

This Court reviews the denial of a preliminary injunction "deferentially for abuse of discretion." *Pope* v. *County of Albany*, 687 F.3d 565, 570 (2d Cir. 2012). A district court abuses its discretion in denying a preliminary injunction "only when the district court decision rests on an error of law or a clearly erroneous finding of fact." *Id.* at 570-71.

ARGUMENT

POINT I

Plaintiffs Have Not Established Standing

Plaintiffs have not demonstrated that any telephony metadata associated with any of their calls ever have been or will ever be reviewed by government personnel, nor have they identified any other injury sufficient to confer standing.

To establish Article III standing, plaintiffs must identify an injury that is "'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Amnesty Int'l*, 133 S. Ct. at 1147 (citations omitted). The Supreme Court has "repeatedly reiterated that 'threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient." *Id.* (quoting *Whitmore* v. *Arkansas*, 495 U.S. 149, 158 (1990)) (alterations and emphasis by the Court); *see also DaimlerChrysler Corp.* v. *Cuno*, 547 U.S. 332, 345 (2006). The "standing inquiry has been especially rigorous when" a plaintiff urges that "an action taken by one of the other two branches of the Federal Government was unconstitutional," and where "the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs." *Amnesty Int'l*, 133 S. Ct. at 1147.

The district court incorrectly concluded that plaintiffs demonstrated standing merely by alleging that business records obtained pursuant to FISC orders included metadata associated with plaintiffs' calls. SPA 17. First, plaintiffs' own allegations demonstrate that their claimed injuries will occur not from the government's possession of such metadata, but rather only if and when government personnel were to review records of plaintiffs' calls. *See*, *e.g.*, JA 23, 24, 26 (alleging that disclosure of plaintiffs' sensitive communications would be harmful); Pl. Br. 1-2, 43 (alleging violation of privacy by government in accessing and examining telephone records), 53 (alleging First

Amendment injury from exposure of "telephonic associations" to the government's "monitoring and scrutiny"). Those asserted harms are not sufficiently alleged or shown here, because—as plaintiffs have not disputed—there is only a speculative prospect that their telephone numbers would ever be used as a selector to query, or be included in the results of queries of, the telephony metadata. Speculation is not a basis for standing. *See Amnesty Int'l*, 133 S. Ct. at 1147-48.

Plaintiffs do suggest in their brief that the government's mere possession of telephony metadata harms them, though they do not allege in their complaint that they suffer any injury from mere possession of metadata. *E.g.*, Pl. Br. 43 (asserting that possession of metadata can reveal "a wealth of detail" about individuals). But plaintiffs do not explain how metadata that no one ever reviews could reveal any details about anyone to the government. The district court correctly observed that the FISC orders establishing the Section 215 program do not permit the government to "conduct[ ] the type of data mining the ACLU warns about in its parade of horribles." SPA 41; *see also* JA 267. The government may review metadata under the Section 215 program only in extremely restricted circumstances that plaintiffs do not contend is likely to implicate information about them. *See* JA 129, 131-32.

Plaintiffs also urge that individuals who would otherwise contact plaintiffs will "likely" be chilled from doing so. JA 26. That "naked assertion," *Iqbal*, 556 U.S. at 678 (internal quotation marks omitted),

based only on speculation about the possible decisions of unnamed third parties to refrain from interacting with plaintiffs, identifies no plausibly impending injury fairly traceable to the conduct of defendants. Rather, such injuries "depend[] on the unfettered choices made by independent actors not before the court[] . . . whose exercise of broad and legitimate discretion the court[] cannot presume . . . to predict." *Lujan* v. *Defenders of Wildlife*, 504 U.S. 555, 562 (1992) (internal quotation marks omitted). And even if there were reason to believe that others would act as plaintiffs assume, any resulting harm would not be attributable to the government's actions, but would be the product of intervening actions by third parties that are not "fairly traceable" to the government's actions under Section 215. *See Amnesty Int'l*, 133 S. Ct. at 1152 & n.7 (citing *Laird* v. *Tatum*, 408 U.S. 1, 10-14 (1972)).

The district court's alternative basis for finding standing (SPA 17) is equally flawed. The court relied on dicta from this Court's opinion in *Amidax Trading Grp.* v. *SWIFT SCRL*, 671 F.3d 140 (2d Cir. 2011), but *Amidax* does not support plaintiffs' standing here. The plaintiff there alleged that its financial information had been turned over to the government, but this Court held that the complaint in that case contained no plausible allegation that had occurred. *Id.* at 148-49. This Court noted the district court's observation that, under the *Amidax* plaintiff's theory of standing, the complaint "need only establish that its information was obtained by the government," and it failed to do so. *Id.* at 147 (internal quotation marks omitted). But there was no occasion to consider

whether such acquisition, if it had been plausibly alleged or proven, would suffice to establish Article III standing.

Here, in contrast, the injuries plaintiffs assert depend not simply on the government's possession of information about them, but rather also on speculation that the government may review information about them and hence "chill" their activities (and the activities of unnamed others) in various respects, or cause some other ill-defined harm. *E.g.*, Pl. Br. 43, 54. The Supreme Court has made clear, however, that the mere fact that the government may have obtained information associated with plaintiffs' telephone calls does not demonstrate standing where, as here, plaintiffs' allegations are premised on a theory of "subjective chill" arising from a speculative fear that the government might "in the future take some other and additional action detrimental to" them with that information. *Laird*, 408 U.S. at 11, 14; *see id.* at 39 (Brennan, J., dissenting).

Plaintiffs suggest that the government "analyze[s] Plaintiffs' call records . . . every time it searches its phone-records database." Pl. Br. 44 n. 11.[6] But plaintiffs fail to explain how they could be harmed by queries of the database unless telephony metadata relating to plaintiffs' calls are responsive to those queries. *See*, *e.g.*, *Amnesty Int'l*, 133 S. Ct. at 114 (requiring

---

[6] Plaintiffs cite no allegations in their complaint to support this argument, and there are none. *See* JA 17-27.

identification of a "concrete, particularized, and actual or imminent" harm that is "fairly traceable" to the conduct complained of (internal quotation marks omitted)). It is no more an injury for a computer query to rule out particular telephony metadata as unresponsive to a query than it would be for a canine sniff to rule out a piece of luggage as nonresponsive to a drug investigation. *See United States* v. *Place*, 462 U.S. 696, 707 (1983) (canine sniff does not violate a reasonable expectation of privacy); *Port Washington Teachers' Ass'n* v. *Board of Educ.*, 478 F.3d 494, 498 (2d Cir. 2007) (injury for Article III standing purposes must be "an invasion of a legally protected interest"). Where telephony metadata associated with particular calls remain unreported and never come to any analyst's attention, there is no meaningful invasion of any cognizable privacy interests, and thus no injury to support plaintiffs' standing to sue.

POINT II

Plaintiffs' Statutory Challenges to the Section 215 Bulk Telephony-Metadata Program Fail

A. Congress Precluded Judicial Review of Plaintiffs' Statutory Claims

The Court should reject plaintiffs' claim that the Section 215 telephony-metadata program exceeds the government's statutory authority. JA 27. In asserting that claim, plaintiffs invoke the Administrative Procedure Act ("APA"), which generally authorizes suit against the federal government for statutory claims seeking non-monetary relief. *See* 5 U.S.C. § 702. APA

review is not available, however, where "any other statute . . . expressly or impliedly forbids the relief which is sought," *id.* § 702, and "where statutes preclude judicial review," *id.* § 701(a)(1). Section 215 precludes plaintiffs from collaterally obtaining judicial review under the APA of whether the FISC correctly held that the Section 215 telephony-metadata program is authorized by statute.

Plaintiffs' statutory claims seek to override the repeated conclusion by the FISC that Section 215 authorizes the government to obtain bulk production from telecommunications companies of business records that consist of telephony metadata in order to assist in counter-terrorism investigations. Section 215 provides that the recipients of such orders may seek judicial review of the orders in the FISC by Article III judges. *See* 50 U.S.C. § 1861(f)(2)(A)(i). Any resulting decision of the FISC is, in turn, reviewable in the FISA Court of Review, also made up of Article III judges, and, ultimately, in the Supreme Court. *See id.* § 1861(f)(3). FISA limits the judicial review of FISC orders issued under Section 215: "Any production or nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect." *Id.* § 1861(f)(2)(D).

Plaintiffs' statutory claims are inconsistent with the framework of judicial review that Congress established in Section 215. The structure of Section 215 confirms that Congress limited judicial review to the FISC and its specialized mechanism for appellate review. The Supreme Court has explained that, "when 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* v. *Cmty. Nutrition Inst.*, 467 U.S. 340, 349 (1984). Congress's decision to create a "precisely drawn, detailed statute pre-empts more general remedies." *United States* v. *Bormes*, 133 S. Ct. 12, 18 (2012) (citation and quotation omitted).

Section 215 contains a detailed, specialized scheme for challenging production orders issued by the FISC, and Congress intended that review mechanism to be exclusive. Section 215 provides for judicial review of such orders only at the behest of "[a] person receiving a production order." 50 U.S.C. § 1861(f)(2)(A)(i). Indeed, recipients of production orders generally may not disclose that the government has obtained such an order. *Id.* § 1861(d)(1). And review proceedings are conducted under specialized security procedures designed to protect sensitive national-security information from disclosure. *See id.* § 1861(f)(3), (4), (5). Plaintiffs are not recipients of the Section 215 production orders they challenge, and they cannot use the more general APA remedy to circumvent the review process carefully crafted by Congress. *See*, *e.g.*, *Block*, 467 U.S. at 346-47 (dairy consumers could not seek APA review under statutory scheme that provided for review only by dairy producers and handlers).

Where Congress did intend to allow private parties to sue the government for FISA violations, it did so expressly. In the same statute that contained Section 215, Congress created a private right of action

against the government. *See* USA PATRIOT ACT, Pub. L. No. 107-56, § 223, 115 Stat. 272, 293 (2001) (codified at 18 U.S.C. § 2712). Congress expressly provided that "aggrieved" persons may sue the United States for damages based on willful violations of the Wiretap Act, the Stored Communications Act, and three particular provisions of FISA that impose restrictions on the use and disclosure of information obtained from electronic surveillance, physical searches, and pen registers or trap and trace devices authorized under FISA. *See* 18 U.S.C. § 2712(a); *see* 50 U.S.C. §§ 1806(a), 1825(a), 1845(a). Congress also made it unlawful for the government to misuse information under Section 215, *see* 50 U.S.C. § 1861(h), but, significantly, did not include that provision among the bases for seeking damages under section 2712, and made no provision whatsoever for the injunctive relief that plaintiffs seek here. These damages remedies are "the exclusive remedy against the United States for any claims within the purview of this section." 18 U.S.C. § 2712(d). Plaintiffs' claims are of the type that are "within the purview" of that section—plaintiffs not only claim that the Section 215 telephony-metadata program violates the Stored Communications Act, *see* Pl. Br. 17-21, but also that the government violated § 1861, a provision of FISA that § 2712 expressly omits from those that form the basis of a cause of action against the government.

Plaintiffs assert that "[t]here is no evidence that Congress's decision to address the review available to the recipients of Section 215 orders was intended to deny judicial review to the subjects of those orders." Pl. Br. 32. Citing legislative history, they suggest

that Congress intended the FISA judicial review provisions to "clarify one species of judicial review, not to extinguish others." Pl. Br. 32. But the report they cite says no such thing. *See* H.R. Rep. 109-174, pt. 1, at 6, 77, 106 (2005). And Congress specifically considered, and rejected, an amendment that would have allowed Section 215 orders to be challenged not only in the FISC, but also in district court. *See id.* at 128-29, 134, 137.

Plaintiffs point to various factual distinctions between this case and the *Block* case that we cite. Pl. Br. 35-37. But the operative legal principle is well-established and not fact-specific: "'[W]hen Congress has dealt in particularity with a claim and [has] intended a specified remedy'—including its exceptions—to be exclusive, that is the end of the matter." *Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians* v. *Patchak*, 132 S. Ct. 2199, 2205 (2012) (quoting *Block* v. *North Dakota* ex rel. *Bd. of Univ. & Sch. Lands*, 461 U.S. 273, 286 n.22 (1983)). There is no support for plaintiffs' suggestion that APA review of Section 215 orders should be permitted simply because Section 215 contains no "administrative-review" requirements; or because plaintiffs' interests may not be perfectly "aligned" with the interests of the recipients of Section 215 production orders. Pl. Br. 35-37. Nor is it surprising that Congress would limit review to challenges brought by recipients of Section 215 orders to produce business records; after all, those recipients are the owners of the business records that are produced to the government under Section 215, *see United States* v. *Miller*, 425 U.S. 435, 440-41 (1976), and are generally the only parties au-

thorized by law to know about these secret production orders.

Under plaintiffs' theory, virtually any customer of a company that received a FISC order could challenge a Section 215 production order in district court—a sweeping proposition that could "'severely disrupt this complex and delicate administrative scheme'" in the sensitive field of intelligence gathering for counter-terrorism efforts. SPA 24 (quoting *Block*, 467 U.S. at 348). Plaintiffs' position would, for example, create the anomalous result that the very same FISC production order could be simultaneously reviewed both in district court and in the FISC. This Court has recognized that it "[i]t is highly unlikely that Congress intended to create a scheme involving multiple avenues of review and potential contradictory results." *Natural Res. Def. Council* v. *Johnson*, 461 F.3d 164, 174 (2d Cir. 2006).

B. The Program Is Authorized by Section 215

Section 215 authorizes the FISC to order the "production of any tangible things" upon the government's application "showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to protect against international terrorism." 50 U.S.C. § 1861(a)(1), (b)(2)(A). The district court recognized that "'[r]elevance' has a broad legal meaning." SPA 33. In civil discovery, it means "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 (1978).

A similarly broad standard of relevance applies to grand jury subpoenas, which may compel production of 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 (1991); *see also EEOC* v. *Shell Oil Co.*, 466 U.S. 54, 68-69 (1984) ("relevance" criteria for administrative subpoenas encompasses "virtually any material that might cast light on the allegations" at issue in an investigation). Applying that common legal understanding of relevance, courts have authorized discovery of large volumes of information where the requester seeks to identify within that volume smaller amounts of information that could directly bear on the matter. *See, e.g.*, *In re Subpoena Duces Tecum*, 228 F.3d 341, 350-51 (4th Cir. 2000); *In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987).

Congress incorporated those usages into Section 215, noting that items subject to production under Section 215 are things obtainable by "a subpoena duces tecum issued by a court . . . in aid of a grand jury investigation" or "any other court order issued by a court . . . directing the production of records or tangible things." 50 U.S.C. § 1861(c)(2)(D); *see, e.g.*, H.R. Rep. No. 109-174, pt. 1, at 131; 152 Cong. Rec. 2426 (Mar. 2, 2006) (statement of Sen. Kyl) ("Relevance is a simple and well established standard of law. Indeed, it is the standard for obtaining every other kind

of subpoena, including administrative subpoenas, grand jury subpoenas, and civil discovery orders"). And, as the FISC has stressed, Section 215's scope is even broader because the statute requires only that the government have "reasonable grounds to believe" that the records sought are relevant to an authorized investigation. *See* 8/29/13 FISC Order at 18.[7] That standard requires deference to the government's reasonable judgments concerning matters that may be relevant.

It is eminently reasonable to believe that Section 215 bulk telephony metadata is relevant to counter-terrorism investigations. The government queries the telephony metadata to identify connections between suspected-terrorist selectors and their unknown contacts. JA 272. Bulk collection of telephony metadata makes it possible to draw those historical connections because there is no way to know in advance which metadata will be responsive to queries for those in contact with suspected-terrorist selectors. JA 276. Absent the creation of a historical repository of information that bulk aggregation of the metadata allows, it may not be feasible under current law for the government to identify chains of communications among known and unknown terrorist operatives that cross different time periods and telecommunications companies' networks. JA 273, 277.

---

[7] The order is available at: http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

Plaintiffs object that only "some small fraction of the records may become useful" to "any specific authorized investigation." Pl. Br. 22 (internal quotation marks omitted). That *ex post* analysis fails to appreciate that, *ex ante*, production in bulk of telecommunications companies' business records permits government analysis that enables discovery of telephone numbers or other metadata of contacts (within one or two steps) of a suspected-terrorist selector. Bulk aggregation of metadata achieves that goal effectively because there is no way to know in advance which numbers suspected terrorist operatives have been in contact with, over which networks, or when. *See* JA 276. The district court correctly pointed out that "courts routinely authorize large-scale collections of information"—such as a computer database—"even if most of it will not directly bear on the investigation." SPA 35. The fact that each particular item of metadata may not generate a lead in an investigation is beside the point.

Plaintiffs acknowledge that "courts have sometimes upheld subpoenas for categories of information," but suggest, without analysis, that telephony metadata "lack[] a sufficient nexus to the investigation they were meant to advance." Pl. Br. 22-23. Plaintiffs overlook that telephony metadata is a "category of relevant data," SPA 36, that does indeed facilitate, and is tied to, specific counter-terrorism investigations. *See* JA 254-55 (providing examples). Plaintiffs' insistence that only a retrospective, case-by-case approach to obtaining business records consisting of telephony metadata is lawful under Section 215, Pl. Br. 23, 50-51, is in tension with that provi-

sion's basic purpose: to facilitate investigations to protect against international terrorism. 50 U.S.C. § 1861(a)(1). In fact, Congress considered and rejected proposals (like those plaintiffs urge here) to limit the use of Section 215 to obtain records pertaining to individuals suspected of terrorist activity. *See* S. 2369, 109th Cong. 2d Sess. § 3 (2006) (unenacted bill that would have required the government to demonstrate that records "pertain to an individual in contact with, or known to, a suspected agent of a foreign power"); *see also* H.R. Rep. No. 109-174, pt. 1, at 129 (statement of Rep. Lungren) ("[t]his is in the nature of trying to stop terrorists before they act, not in the nature of a regular criminal investigation"). Congress did not adopt that narrow, retrospective approach, and instead codified a broad concept of relevance that permits a broader kind of intelligence gathering that facilitates national security investigations to prevent international terrorism, and not only after-the-fact criminal investigations of such conduct. *See* JA 252.

Plaintiffs declare that "[t]he government's argument simply has no limit" because if the government can obtain telephony metadata in bulk, then "many other sets of records" would be susceptible of bulk collection. Pl. Br. 25. But the question of relevance cannot be assessed in the abstract because it is so "variable in relation to the nature, purposes, and scope of [an] inquiry." *Oklahoma Press Pub. Co.* v. *Walling*, 327 U.S. 186, 209 (1946). And plaintiffs' objection does not undermine the relevance of bulk telephony metadata to counter-terrorism investigations, as described above. *E.g.*, JA 272-74. Communications records have characteristics—specifically their highly

standardized and interconnected nature—that make them readily susceptible to analysis in large datasets to bring previously unknown connections between and among individuals to light. The same cannot be said of all other types of records.

Contrary to plaintiffs' suggestion, Pl. Br. 25-26, it is not surprising that Congress codified a broad concept of relevance, given the significant statutory protections Congress built into Section 215 that are not present in other contexts. Unlike civil discovery, grand jury subpoenas, or national security letters, Section 215 orders always require prior judicial approval of, among other things, the government's assertion that the business records are relevant. 50 U.S.C. § 1861(a)(1). Information about U.S. persons obtained under Section 215 may be retained and disseminated only in accordance with minimization procedures approved by the FISC. *See id.* § 1861(g). And the process is subject to internal, inter-agency, judicial, and congressional regulation and oversight. *Id.* § 1862; JA 269.

Finally, Congress has reaffirmed the broad concept of relevance embodied in Section 215 by twice reauthorizing the statute—in 2010 and 2011—after receiving extensive and detailed classified briefings informing legislators that the government and the FISC had interpreted Section 215 to permit the bulk telephony-metadata program. *See* JA 148-173; *see al-*

so 8/29/13 FISC Order at 23-27;[8] JA 312. The Supreme Court has observed in a similar context that "Congress undoubtedly was aware of the manner in which the courts were construing the concept of 'relevance' and implicitly endorsed it by leaving intact the statutory definition." *EEOC* v. *Shell Oil Co.*, 466 U.S. 54, 69 (1984); *see also Forest Grove School Dist.* v. *T.A.*, 557 U.S. 230, 239-40 (2009) ("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." (internal quotation marks omitted))

Plaintiffs dismiss the significance of legislative reauthorization, arguing that the government did not provide any "legal analysis" to Congress in the classified briefings describing the Section 215 telephony-metadata program. Pl. Br. 27. But congressional ratification does not depend on whether Congress agreed with the government's (or the FISC's) legal analysis. Nor does ratification turn on the number of legislators with actual knowledge of the government's interpretation, or whether they shared classified information with staff. Pl. Br. 27-28. The government has repeatedly and faithfully kept Congress informed about the Section 215 bulk telephony-metadata program. JA 175. The Supreme Court has never required the sort of showing that plaintiffs demand before concluding that Congress ratified an interpretation of

---

[8] The order is available at: http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

prior law by reenacting it. *See Shell Oil*, 466 U.S. at 69 & n.21; *Haig* v. *Agee*, 453 U.S. 280, 297-98 & n.37 (1981) (finding "clear" and "undoubted" congressional awareness of judicial and executive interpretations based on references in committee reports).

C. The Program Does Not Violate the Stored Communications Act

There is no merit to what plaintiffs apparently now consider the centerpiece of their statutory arguments—that the Stored Communications Act prohibits the government from obtaining any business records about telephone subscribers pursuant to Section 215. Pl. Br. 17-21. As explained above, a damages suit is the "exclusive remedy against the United States" for violations of the Stored Communications Act, 18 U.S.C. § 2712(d), and plaintiffs apparently agree. *See* Pl. Br. 30. That exclusive remedy precludes plaintiffs' claims for injunctive relief here.

But even apart from preclusion, Congress did not prohibit the government from obtaining telephony metadata under Section 215. If plaintiffs' interpretation were correct, the government would have no means under Section 215 to issue even the "targeted demands" for telephone-subscriber information that plaintiffs apparently believe are the only lawful means of intelligence-gathering in this field. Pl. Br. 50. Given the frequent use of the international telephone system by terrorist networks, *see* JA 261, it would be remarkable if Congress had forbidden the government from obtaining any telephone records in a statute designed to provide investigative tools for

counter-terrorism investigations—especially given that it twice reenacted the statute without any suggestion of conflict with the Stored Communications Act. *See supra*, 35-36.

Section 215 broadly permits the FISC to order the production of "any tangible things" "to obtain foreign intelligence information" or "to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(a)(1). The term "any" must be given "an expansive meaning" absent language explicitly "limiting" it. *United States* v. *Gonzales*, 520 U.S. 1, 5 (1997). There is no serious doubt that the records at issue here fall within the statutory term "any tangible things."

There is no indication that Congress intended the Stored Communications Act—which provides that telecommunications companies generally may not disclose information pertaining to a subscriber to the government, *see* 18 U.S.C. § 2702(a)(3)—to limit the broad language of Section 215. Plaintiffs urge that Section 215 is not "an implicit exception to" § 2702. Pl. Br. 18. But plaintiffs' argument would require the Court to find that the Stored Communications Act is an implicit exception to, or limit on, the expansive authorization for production of "any tangible things" under Section 215. The FISC has observed that, "[i]f the above-described statutory provisions are to be reconciled, they cannot all be given their full, literal effect." JA 334. The Court's task, then, is to harmonize these statutory directives to reflect Congress's intent. *See FDA* v. *Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000).

Here, as the FISC has correctly concluded, FISA's structure makes clear that Congress did not intend other statutory restrictions on disclosure, such as the Stored Communications Act, to limit the reach of Section 215. *See* JA 337. Section 215 requires high-level government authorization before the government seeks authority from the FISC to obtain "tax return records, educational records, or medical records containing information that would identify a person." 50 U.S.C. § 1861(a)(3).[9] The disclosure of those categories of records is independently regulated by other statutes. *See* 26 U.S.C. § 6103(a) (tax records); 20 U.S.C. § 1232g(b)(1) (educational records); 42 U.S.C. § 1320d-6 (medical records). Section 215's reference to those types of records confirms that they are within Section 215's general authorization for the production of tangible things, regardless of other statutory restrictions. By the same token, Section 215 permits acquisition of information that would be obtainable "with any other order issued by a court of the United States." 50 U.S.C. § 1861(c)(2)(D). Records subject to the Stored Communications Act's restrictions are obtainable through court order. *See* 18 U.S.C. § 2703(d). These provisions demonstrate that Congress did not intend the Stored Communications Act to restrict the universe of "any tangible things" that the FISC may order produced under Section 215, 50 U.S.C. § 1861(a).

---

[9] Congress rejected a proposal to subject Section 215 production orders to other statutory restrictions on disclosure. *See* 147 Cong. Rec. 19530-33 (2001).

Plaintiffs concede that the government may obtain tax records, educational records, and medical records under Section 215, "despite applicable confidentiality provisions elsewhere." *See* Pl. Br. 19. The same interpretation permits obtaining telephony metadata because Section 215's sweeping authorization for the production of "any tangible things," 50 U.S.C. § 1861(a)(1), makes no distinction between telephony metadata and the other kinds of records that plaintiffs agree may be produced under Section 215. *See Clark* v. *Martinez*, 543 U.S. 371, 378 (2005). Plaintiffs argue that the additional requirements for disclosure of tax records, educational records, and medical records mean that Congress intended those sorts of information—but not telephony metadata—to be free of other restrictions on disclosure. Pl. Br. 19-20. That argument gets things exactly backwards: the fact that Congress did not subject telephony metadata to additional restrictions only underscores the broader scope of the FISC's authority under Section 215 to order production of that information—an unsurprising result given the more substantial privacy interests implicated by tax records, educational records, and medical records.

The statute authorizing FBI national security letters (NSLs) reinforces this interpretation. The FBI may issue an NSL without prior judicial review, and compel a telephone service provider to produce "subscriber information and toll billing records information," based on the FBI's certification that the records are relevant to an authorized terrorism investigation. 18 U.S.C. § 2709(a). It would be passing strange if Congress had permitted the government to

obtain telephony metadata through NSLs without prior judicial review under § 2709, only to prohibit the government categorically from obtaining any telephony metadata whatsoever under the comprehensive system of judicial authorization and supervision established by Section 215.

POINT III

The Section 215 Bulk Telephony-Metadata Program Does Not Violate Plaintiffs' Constitutional Rights

A. The Program Does Not Violate Plaintiffs' Fourth Amendment Rights

1. The Program Does Not Infringe a Constitutionally Protected Privacy Interest

The Supreme Court has rejected the premise of plaintiffs' Fourth Amendment argument, holding that there is no reasonable expectation of privacy in the telephone numbers dialed in order to connect a telephone call. In *Smith*, the Supreme Court held that the government's recording of the numbers dialed from an individual's home telephone, through the offsite installation of a pen register, does not constitute a search under the Fourth Amendment. *Smith*, 442 U.S. at 743-44. The FISC has correctly relied on the holding of *Smith* to conclude that the acquisition from telecommunications companies of business records consisting of bulk telephony metadata is not a search

for purposes of the Fourth Amendment. *See* JA 313; 8/29/13 FISC Order at 6.[10]

Smith is based on fundamental Fourth Amendment principles. First, the Court recognized that, because the government ascertained the numbers dialed from a particular telephone by installing equipment "on telephone company property," the petitioner there "obviously [could not] claim that his 'property' was invaded or that police intruded into a 'constitutionally protected area.'" *Smith*, 442 U.S. at 741. The Court also contrasted the collection of the numbers dialed with a listening device that would permit the government to monitor the content of communication. *Id.* ("a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications" (emphasis the Court's)). Thus, the only Fourth Amendment issue in *Smith* was whether a telephone user has a reasonable expectation of privacy in the numbers he dials. Because telephone users convey numbers to the telephone company to complete their calls, and because the telephone company can and does routinely record those numbers for legitimate business purposes, the Court held that any "subjective expectation that the phone numbers [an individual] dialed would remain private . . . is not one that society is prepared to recognize as reasonable." *Id.* at 743 (internal quotation marks omitted).

---

[10] The order is available at: http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

In so holding, the *Smith* Court reaffirmed the established principle 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. Just as "a bank depositor has no legitimate expectation of privacy in financial information voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business," a telephone user has no expectation that conveying a telephone number to the company will protect that number from further disclosure. *Id.* at 744 (internal quotation marks omitted).

The third-party doctrine reaffirmed in *Smith* creates a readily discernible bright-line rule establishing what is, and is not, protected under the Fourth Amendment. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 564 (2009), *cited in* SPA 39 n.16. It would be nearly impossible for government officials to divine on a case-by-case basis whether an individual might have an expectation of privacy in particular information that the person has conveyed to a third party, and certainty is essential in this area to facilitate compliance with the Constitution. *Id.* at 581-86.

Like the FISC, the district court here correctly recognized that *Smith* precludes plaintiffs' Fourth Amendment claims. SPA 39-42. Indeed, the Fourth Amendment concerns here are even weaker than in *Smith*. Unlike a pen register, which intercepts the transmission of information from a subscriber to a telecommunications company, the FISC orders here direct specific telecommunications companies to pro-

vide the government with the companies' own business records that they maintain for their own business purposes. Plaintiffs have no reasonable expectation of privacy in corporate business records, even if those records reflect transactions in which they were involved.

Smith remains the law, and its principles have guided Fourth Amendment decisions even in the Internet Age. The courts of appeals have recognized, for example, that there is no reasonable expectation of privacy in information conveyed to a third party even when using forms of communication that did not exist when the Supreme Court handed down *Smith*. *See*, *e.g.*, *United States* v. *Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008) (email "to/from" and Internet Protocol addressing information); *Quon* v. *Arch Wireless Operating Co.*, 529 F.3d 892, 905 (9th Cir. 2008) (text message address information), *rev'd on other grounds*, 560 U.S. 746 (2010); *Guest* v. *Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001) (subscriber information such as names, addresses, birthdates, and passwords communicated to systems operations and Internet service providers). This Court has similarly recognized that, while "[i]ndividuals generally possess a reasonable expectation of privacy in their home computers," there is no such "expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient." *United States* v. *Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (citing *Guest*, 255 F.3d at 333). This case is far easier: it involves telephony metadata, the same kind of data that was at issue in *Smith*.

Plaintiffs argue that *Smith* can be disregarded. Pl. Br. 39-43. But the district court correctly recognized that "the Supreme Court has instructed lower courts not to predict whether it would overrule a precedent," and "[i]nferior courts are bound by th[e] precedent" of *Smith*. SPA 43 (citing *Agostini* v. *Felton*, 521 U.S. 203, 237 (1997); *Rodriguez de Quijas* v. *Shearson/Am. Express, Inc.*, 490 U.S. 477, 484 (1989)).

The notion that the Section 215 program implicates a Fourth Amendment privacy interest is particularly implausible given the type of information obtained under the program. The governing FISC orders require specified telecommunications companies to turn over only limited information from their business records under Section 215; that telephony metadata does not include the identity of any particular subscriber or called party. JA 246-250, 263, 264-65; SPA 41. The FISC orders only permit access to telephony metadata that is within two steps of a selector for which there is a reasonable, articulable suspicion (now founded on a prior judicial determination) of association with a terrorist organization. JA 251, 264, 266; 2/5/14 FISC Order at 4-9. Plaintiffs are therefore wrong to claim that the Section 215 program could indiscriminately yield a "wealth of detail" about individuals. Pl. Br. 43. In any event, the Supreme Court in *Smith* considered and rejected the very concerns plaintiffs now urge. *See Smith*, 442 U.S. at 748 (Stewart, J., dissenting). The checks, deposit slips, and other customer bank records at issue in *Miller*—a case on which *Smith* relied—surely revealed personal details. *See id.* at 743 (citing *Miller*, 425 U.S. at 442-44).

Second, plaintiffs argue that *Smith* does not control because of the "mass" or "dragnet" nature of the government activity alleged here. Pl. Br. 40. But Fourth Amendment rights "are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched." *Steagald* v. *United States*, 451 U.S. 204, 219 (1981); *accord*, *e.g.*, *Minnesota* v. *Carter*, 525 U.S. 83, 88 (1998); *Rakas* v. *Illinois*, 439 U.S. 128, 133-34 (1978).[11] Under *Smith*, no caller has a reasonable expectation of privacy in telephone numbers he dials. Plaintiffs cannot prevail by purporting to aggregate the (nonexistent) Fourth Amendment interests of others, no matter how numerous. Thus, the district court rightly rejected plaintiffs' arguments regarding the asserted Fourth Amendment implications of so-called "mass surveillance." SPA 42-43. Other courts have rejected arguments that are materially indistinguishable from plaintiffs' here. *See*, *e.g.*, *In re Grand Jury Proceedings*, 827 F.2d at 305 (rejecting argument that a sub-

---

[11] Thus, plaintiffs, who have not shown that metadata about their calls have been reviewed by government personnel, cannot invoke the Fourth Amendment rights of others, even if there were a reasonable expectation of privacy in telephony metadata. *See*, *e.g.*, *Rakas*, 439 U.S. at 138; *United States* v. *Haqq*, 278 F.3d 44, 47 (2d Cir. 2002) (an individual's Fourth Amendment rights are violated only when the challenged conduct invaded his own legitimate expectation of privacy rather than that of a third party).

poena was unreasonable under the Fourth Amendment because it "may make available . . . records involving hundreds of innocent people"); *United States* v. *Rigmaiden*, 2013 WL 1932800, at *13 (D. Ariz. May 8, 2013) (no Fourth Amendment violation when government acquired 1.8 million IP addresses).[12] Similarly, the FISC has correctly recognized that "where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*." 8/29/13 FISC Order at 9.

Plaintiffs also invoke cases involving physical surveillance of individuals. Pl. Br. 40-42 (citing *United States* v. *Knotts*, 460 U.S. 276 (1983), and *United States* v. *Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd on other grounds sub nom. United States* v. *Jones*, 132 S. Ct. 945 (2012)). But those cases do not support plaintiffs' arguments here. In 1983, the Supreme Court declined to decide whether warrantless electronic tracking of a suspect's car could become

---

[12] For these reasons, plaintiffs' Fourth Amendment claims fail regardless of the scope of the business records obtained under the program. Plaintiffs' mistaken belief, also reflected in the district court's description in its opinion, that the Section 215 bulk telephony-metadata program includes all or virtually all of the telephony metadata of Americans thus does not alter the result here. *See supra*, 6-7. Many details of the program remain classified, but that cannot justify unsupported assumptions.

constitutionally problematic if extended to "twenty-four hour surveillance of any citizen." *Knotts*, 460 U.S. at 283 (internal quotation marks omitted). In 2012, the Court again declined to endorse the view that extended electronic tracking necessarily implicates greater Fourth Amendment concerns than other surveillance. *Jones*, 132 S. Ct. 945-46. The decision of the Court in *Jones* turned not on the pervasiveness of the surveillance at issue, but on the attachment of a GPS device to a vehicle, which was a physical intrusion or trespassory interference with an individual's property, violating core Fourth Amendment protections unrelated to the duration of the resulting surveillance. *Compare Jones*, 132 S. Ct. at 949 ("The Government physically occupied private property for the purpose of obtaining information"), *with Smith*, 442 U.S. at 741 (noting that obtaining call record information from telephone company facilities does not implicate an individual's rights in his own property). Here, the situation is the converse of *Jones*: plaintiffs are asserting a Fourth Amendment interest in records owned not by them, but rather by telecommunications companies.

Plaintiffs rely on two concurring opinions in *Jones* to speculate that the Supreme Court might decide *Smith* differently now. Pl. Br. 41-43. But the majority opinion in that case is the governing law, and the Court there articulated no reason to displace or modify *Smith*. In any event, the concerns voiced by some concurring Justices in *Jones* do not apply to the Section 215 telephony-metadata program.

Plaintiffs focus, in particular, on the concurring opinion of Justice Sotomayor, which noted that continuous GPS monitoring "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring). Unlike the GPS data at issue in that case, however, the FISC orders underlying the Section 215 telephony-metadata program do not permit the indiscriminate compilation of detail about anyone; rather, the information in the database may be reviewed only as part of the highly restricted process of querying.

Given the conclusive, controlling effect of *Smith*, the district court correctly dismissed plaintiffs' Fourth Amendment claims for failure to state a claim.

2. If Obtaining Metadata Implicated a Fourth Amendment Privacy Interest, the Program Would Still Be Constitutional

If obtaining bulk telephony metadata from the business records of telecommunications companies implicated a Fourth Amendment privacy interest, it would nevertheless be constitutionally permissible. The Fourth Amendment bars only unreasonable searches and seizures, and the Section 215 telephony-metadata program is reasonable under the standard applicable to searches that serve "special needs" of the government. *See*, *e.g.*, *Cassidy* v. *Chertoff*, 471 F.3d 67, 75 (2d Cir. 2006) ("'[T]he ultimate measure

of the constitutionality of a governmental search is 'reasonableness.'") (quoting *Vernonia Sch. Dist. 47J* v. *Acton*, 515 U.S. 646, 652 (1995)). The national security and safety interests served by the Section 215 program are special needs. *See Cassidy*, 471 F.3d at 82; *MacWade* v. *Kelly*, 460 F.3d 260, 270-71 (2d Cir. 2006) (citing *Michigan Department of State Police* v. *Sitz*, 496 U.S. 444 (1990)).

Plaintiffs acknowledge that this "special needs" standard applies if compliance with "the warrant and probable-cause requirement" is "impracticable." Pl. Br. 47 (internal quotation marks and citations omitted). That standard governs here because, as the government has shown and as the FISC has repeatedly concluded, the Section 215 bulk telephony-metadata program provides an efficient means to identify otherwise-unknown contacts (at one or two steps of contact) of telephone numbers and other selectors that are reasonably suspected of being used by terrorist organizations, including connections that retrospective analysis can make evident in calls that occurred before the relevant terrorist connection became known. The Section 215 bulk telephony-metadata program provides the government with a historical repository of metadata cutting across multiple providers that permits contact chaining and additional analysis that could not be accomplished as effectively, if at all, with more targeted investigative tools, such as probable-cause warrants. JA 252-56, 272-77.

The question, then, is whether the program is reasonable, *see* U.S. Const. amend. IV, and it is. That standard requires balancing "the promotion of legiti-

mate governmental interests against the degree to which [any search] intrudes upon an individual's privacy." *Maryland* v. *King*, 133 S. Ct. 1958, 1970 (2013) (internal citation and quotation marks omitted). The interest in preventing international terrorist attacks by identifying and tracking terrorist operatives is a national security concern of overwhelming importance. *See Agee*, 453 U.S. at 307 ("no governmental interest is more compelling" than national security); *In re Directives*, 551 F.3d 1004, 1012 (FISC-R 2008) ("the relevant governmental interest—the interest in national security—is of the highest order of magnitude"). The Section 215 bulk telephony-metadata program enhances the government's ability to uncover and monitor unknown terrorist operatives who could otherwise elude detection, and has meaningfully contributed to counter-terrorism investigations. JA 246, 251-55, 260-61, 272-77.

Any Fourth Amendment privacy interest implicated by the Section 215 program, in contrast, is minimal. The governing FISC orders strictly limit analysis of the metadata, and there is no non-speculative basis to believe that any information concerning plaintiffs' calls has been or will ever be seen by any person. JA 99-109, 262-69; 2/5/14 FISC Order. *See King*, 133 S. Ct. at 1979 (finding no Fourth Amendment violation where safeguards limiting DNA analysis to identification information alone reduced any intrusion into privacy); *Board of Educ.* v. *Earls*, 536 U.S. 822, 833-34 (2002) (no Fourth Amendment violation where restrictions on access to drug testing results lessened intrusion on privacy); *Vernonia Sch. Dist.*, 515 U.S. at 658 (no Fourth Amendment viola-

tion where student athletes' urine was tested for illegal drugs and not for any medical condition); *Sitz*, 496 U.S. at 450-51 (no Fourth Amendment violation where safety interests served by drunk driving checkpoints outweighed motorists' interests in driving without being stopped).

The record amply establishes that the Section 215 bulk telephony-metadata program, coupled with the targeted and judicially supervised querying of that metadata, is at least a "reasonably effective means" of promoting the government's national security objectives. *Earls*, 536 U.S. at 837. Indeed, this Court has upheld searches on national security grounds that were arguably more intrusive. *See Cassidy*, 471 F.3d at 70 (searches of carry-on luggage and vehicles before boarding ferries); *MacWade*, 460 F.3d at 270-71 (random search of subway passengers' baggage).

Plaintiffs downplay the importance of the Section 215 telephony-metadata program. Pl. Br. 2, 50-51. The record, however, reflects the views of government officials that the program is a valuable counterterrorism tool. *E.g.*, JA 248, 255-56, 277-78. The President also has stressed the "importance of maintaining this capability." 3/27 President Statement. The courts owe deference to the assessment of the Executive Branch, not to plaintiffs' contrary views. *See*, *e.g.*, *Holder* v. *Humanitarian Law Project*, 130 S. Ct. 2705, 2727 (2010); *Wilner* v. *NSA*, 592 F.3d 60, 76 (2d Cir. 2009). The political branches continue to debate the best means to accomplish the important goals of Section 215, and the program may continue to be modified to reflect those policy decisions. *See*, *e.g.*, 3/27

President Statement; 3/28 AG-DNI Joint Statement. But those debates do not support plaintiffs' constitutional arguments, nor do they disprove the importance of the Section 215 program.

Plaintiffs also argue that the Section 215 telephony-metadata program is an impermissible "general search predicated on a general warrant." Pl. Br. at 46, 50. The program is not a search at all; but even if it were, it is certainly nothing like a general warrant, which is one that permits the government to search for evidence of unlawful activity in unspecified places or for unspecified things. *See Steagald* v. *United States*, 451 U.S. 204, 220 (1981). The cases plaintiffs cite involved the authorization of electronic eavesdropping into the content of private conversations, a far greater intrusion on privacy interests than the Section 215 bulk telephony-metadata program. *See* Pl. Br. 46-50 (citing *Berger* v. *State of New York*, 388 U.S. 41 (1967); *United States* v. *U.S. Dist. Court (Keith)*, 407 U.S. 297 (1972); *United States* v. *Tortorello*, 480 F.2d 764 (2d Cir. 1973); *United States* v. *Cafero*, 473 F.2d 489 (3d Cir. 1973)). *Smith* highlighted the difference between obtaining telephony metadata and the surveillance of communications content. 442 U.S. at 741. And the Section 215 program at issue here does not involve electronic surveillance; the FISC orders require only the production of providers' business records. Thus, plaintiffs' invocation of a heightened standard of reasonableness in the context of electronic surveillance is inapplicable here.

B. The Program Does Not Infringe Plaintiffs' First Amendment Rights

Plaintiffs err in contending that the Section 215 telephony-metadata program violates their First Amendment rights. "'[I]ncidental burdens on the right to associate do not violate the First Amendment,'" and any First Amendment claim therefore must be based on an interference with plaintiffs' associational rights that is "direct and substantial" or "significant." SPA 46 (quoting *Tabbaa* v. *Chertoff*, 509 F.3d 89, 101 (2d Cir. 2007) (internal quotation marks omitted)). Plaintiffs cannot satisfy that standard. The governing FISC orders require production of telecommunication service companies' business records consisting of telephony metadata. For the same reasons that plaintiffs lack a Fourth Amendment privacy interest in such information, any marginal burden on plaintiffs' alleged right of "associational privacy," Pl. Br. 58, is incidental. Moreover, as the district court observed, plaintiffs' alleged injury could arise only if a person actually reviewed telephony metadata associated with a telephone call involving plaintiffs. *See* SPA 46-47; *see also* Pl. Br. 54. Plaintiffs do not dispute that such a possibility is speculative, and they do not explain how they could suffer any substantial burden solely from the alleged fact that the government obtains business records including telephony metadata if no analyst ever sees any data involving

plaintiffs, and if the records themselves contain no personally identifying information. Pl. Br. 58.[13]

Plaintiffs point to cases involving targeted, compelled disclosure of the membership rolls of expressive organizations. Pl. Br. 56 (citing *Bates* v. *City of Little Rock*, 361 U.S. 516 (1960), and *Gibson* v. *Florida Leg. Investigation Comm.*, 372 U.S. 539 (1963)). But there is no suggestion that the Section 215 bulk telephony-metadata program singles out plaintiffs or others in any way, let alone on the basis of expressive activity; indeed, plaintiffs' central objection to the program is that it allegedly obtains information indiscriminately. Government investigative activities that lack any purpose to suppress expression or association do not violate the First Amendment. *See Reporters Comm. for Freedom of the Press* v. *AT&T*, 593 F.2d 1030, 1051-52 (D.C. Cir. 1978).

---

[13] Like the district court, SPA 45-46, this Court need not address whether plaintiffs have a separate First Amendment claim, apart from their Fourth Amendment arguments. See, *e.g.*, *Gordon* v. *Warren Consol. Bd. of Educ.*, 706 F.2d 778, 781 n.3 (6th Cir. 1983) (collecting cases) ("surveillance consistent with Fourth Amendment protections . . . does not violate First Amendment rights, even though it may be directed at communicative or associative activities"); SPA 45 ("[t]he Government's argument is well-supported").

POINT IV

The District Court Correctly Denied Plaintiffs' Motion for a Preliminary Injunction

For the reasons stated above, plaintiffs cannot establish a likelihood of success on the merits of their statutory or constitutional claims. They also cannot establish the other required elements of a preliminary injunction, namely "that [they are] likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in [their] favor, and that an injunction is in the public interest." *Winter* v. *Natural Res. Def. Council*, 555 U.S. 7, 20 (2008).

Plaintiffs have failed to show that they will be irreparably harmed absent preliminary injunctive relief. Plaintiffs incorrectly contend that irreparable injury may be "presumed" in cases alleging constitutional deprivations. Pl. Br. 60. That argument is inconsistent with Supreme Court cases and this Court's precedent, which make clear that "courts must not simply presume irreparable harm." *Salinger* v. *Coating*, 607 F.3d 68, 82 (2d Cir. 2010) (citing *eBay, Inc.* v. *MercExchange, LLC*, 547 U.S. 388 (2006)).

The district court also correctly concluded that "the balance of the equities and the public interest tilt firmly in favor of the Government's position." SPA 47. The particular public interest at issue here—the government's interest in combating international terrorism and protecting the national security of the United States—is "an urgent objective of the highest order." *Humanitarian Law Project*, 130 S Ct. at 2724; *see also*, *e.g.*, *Agee*, 453 U.S. at 307 ("no governmental

interest is more compelling than the security of the Nation"). The district court held that "[a]ny injunction dismantling the section 215 telephony-metadata collection program 'would cause an increased risk to national security and the safety of the American public.'" SPA 48 (quoting JA 277). That finding was firmly rooted in the record. SPA 48-49 (discussing examples).

Plaintiffs rely instead on what they take to be the assessment of the Section 215 bulk telephony-metadata program in reports by the President's Review Group (PRG) and the Privacy and Civil Liberties Oversight Board (PCLOB). Pl. Br. 61. Plaintiffs misunderstand the conclusions of those groups, which do not in any event overcome the evidence in the record reflecting the experience of the President and those charged with defending national security in this sensitive area. Both the PRG and the PCLOB recognized the utility of the Section 215 bulk telephony-metadata program, but concluded that the program was not "essential" in light of other investigatory tools. *See*, *e.g.*, PRG Report at 104.[14] The PCLOB likewise acknowledged that the Section 215 bulk telephony-metadata program has value. PCLOB Report at 146.[15] Those reports inform the ongoing debate within the political branches, but are no basis for reversing the district court's assessment of the record

---

[14] The report is available at: http://1.usa.gov/1cBct0k.

[15] The report is available at: http://bit.ly/1d01flI.

in this case, especially in light of the President's most recent statement reaffirming the importance of this capability, and the need for the program to continue while Congress considers legislation that could replace the program with an effective alternative. *See supra*, 52.

Finally, the injunction plaintiffs seek is impractical and would pose substantial burdens, even if it were otherwise permissible. The injunctive relief at issue—(1) barring the government from obtaining telephony metadata of calls involving plaintiffs; (2) requiring a quarantine of telephony metadata of calls involving plaintiffs; and (3) prohibiting the government from querying Section 215 telephony metadata using any telephone number or other selector associated with plaintiffs—would require the NSA to somehow identify all such selectors that belong to or are associated with plaintiffs. JA 278. Even if plaintiffs were to provide such selectors, it would be extremely burdensome to implement the requested injunction.[16]

---

[16] The record includes information from the NSA explaining the technical hurdles: The agency would need to develop the technical capability to remove specified numbers from the database upon receipt of each batch of provider records, or to block the numbers from view when the database is queried. Developing that capability would likely require hiring additional personnel and could take months. Moreover, if the injunction were later lifted, the NSA would have to devise a way to reverse that capability, which would require additional resources. JA 278.

Moreover, the requested injunction would also require the government to access the metadata beyond the limits imposed by the current FISC orders authorizing the program.

The district court correctly assessed that the public interest and the balance of the equities strongly militate against issuance of a preliminary injunction. That assessment was not an abuse of discretion.

CONCLUSION

For the foregoing reasons, the judgment of the district court should be affirmed.

Dated: New York, New York
April 10, 2014

Respectfully submitted,

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

STUART F. DELERY,
Assistant Attorney General,

Attorneys for Defendants-Appellees.

DAVID S. JONES,
JOHN D. CLOPPER,
EMILY E. DAUGHTRY,
Assistant United States Attorneys,
DOUGLAS N. LETTER,
H. THOMAS BYRON III,
HENRY C. WHITAKER,
Attorneys, Appellate Staff,
Civil Division, U.S. Department of Justice,
Of Counsel.

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 32(a)(7)(C) of the Federal Rules of Appellate Procedure, the undersigned counsel hereby certifies that this brief complies with the type-volume limitation of Rule 32(a)(7)(B). As measured by the word processing system used to prepare this brief, there are 13,338 words in this brief.

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

By: DAVID S. JONES,
Assistant United States Attorney