No. _____

In The

Supreme Court of the United States

LARRY KLAYMAN, CHARLES STRANGE,
and MARY ANN STRANGE,

Petitioners,

v.

BARACK HUSSEIN OBAMA, II,
ERIC H. HOLDER, JR., KEITH B. ALEXANDER,
ROGER VINSON, NATIONAL SECURITY AGENCY,
and U.S. DEPARTMENT OF JUSTICE,

Respondents.

On Petition For A Writ Of Certiorari Before Judgment To The United States Court Of Appeals For The District Of Columbia Circuit

PETITION FOR WRIT OF CERTIORARI BEFORE JUDGMENT

LARRY KLAYMAN, ESQ.
2020 Pennsylvania Ave. NW, #345
Washington, DC 20006
Tel: (310) 595-0800
Email: leklayman@gmail.com

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

QUESTION PRESENTED

Whether the National Security Agency ("NSA") Respondents' indiscriminate collection and access to telephonic metadata on nearly the entire U.S. citizenry, without regard to there being probable cause of any connection to terrorists or terrorism, constitutes an unreasonable search and seizure violative of the Fourth Amendment to the U.S. Constitution?

PARTIES TO THE PROCEEDINGS

Petitioners, who were Plaintiffs below, are Larry Klayman, Charles Strange, and Mary Ann Strange. Respondents, which were Defendants below, are Barack Hussein Obama, II, Eric H. Holder, Jr., Keith B. Alexander, Judge Roger Vinson, the NSA, and the U.S. Department of Justice.

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

Page

TABLE OF AUTHORITIES – Continued

Page

When the people fear the Government, there is tyranny – Thomas Jefferson

PETITION FOR WRIT OF CERTIORARI BEFORE JUDGMENT

Petitioners respectfully petition this Court for a writ of certiorari to review a case still pending in the U.S. Court of Appeals for the District of Columbia Circuit, before final judgment is entered. On December 16, 2013, the Honorable Richard J. Leon of the U.S. District Court for the District of Columbia (hereinafter "district court") issued a preliminary injunction ordering certain named Government Defendants to:[1]

> "I will grant Larry Klayman's and Charles Strange's requests for an injunction[ ] and enter an order that (1) bars the Government from collecting, as part of the NSA's [National Security Agency's] Bulk Telephony Metadata Program, any telephony metadata associated with their personal Verizon accounts and (2) requires the Government to destroy any such metadata in its possession that was collected through the bulk collection program.[ ]"

---

[1] The district court's order defined the Government Defendants as "several federal agencies and individual executive officials," including Barack Hussein Obama, II, Eric H. Holder, Jr., Keith B. Alexander, Judge Roger Vinson, the National Security Agency (NSA), and the U.S. Department of Justice. App. 4, 5. (Collectively referred to as NSA Respondents).

Judge Leon's Memorandum Opinion of December 16, 2013 at 67 (App. 88). Judge Leon, however, stayed his order pending appeal, " . . . in light of the significant national security interests at stake in this case and the novelty of the constitutional issues."[2] App. 10.

This case is of such imperative public importance that it justifies deviation from normal appellate practice and requires immediate consideration and determination in the Supreme Court. Specifically, as testified to below by Dr. Edward W. Felten, Professor of Computer Science and Public Affairs, as well as Director of the Center for Information Technology Policy, at Princeton University, the Government Defendants' overly broad, unwarranted, and unlawful access to and collection of domestic telephonic metadata, unjustifiably allows them to track even the most intimate details of an individual's life, providing them information as to a person's associations, political and religious beliefs, social activities, and even their location at a given time. The Fourth Amendment rights of over 300 million American citizens with no probable cause of communications to terrorists

[2] Judge Leon recognized that his preliminary injunction order would ultimately be before the Supreme Court. He stated at oral argument on November 18, 2013, "I know what's going to happen here no matter how I rule, it is going to the Court of Appeals and it probably will go to the Supreme Court after that, at least certainly one side or the other. It doesn't matter however I rule . . . However I come out, I know it is going upstairs." Transcript of Oral Argument on November 18, 2013 at pg. 52.

or terrorism as required for a relevant investigation under Section 215 (50 U.S.C. § 1861) and Section 702 (50 U.S.C. § 1881a), have been and continue to be violated by the National Security Agency and other Government Defendants (hereinafter "NSA Respondents") in spite of and in the face of the court's December 16, 2013 order.

Two district courts, in two different circuits, the District of Columbia and the Southern District of New York, and the secret Foreign Intelligence Surveillance Court (FISC), have recently reached contrary decisions over whether the actions of the NSA Respondents and their overreaching surveillance tactics violate the Fourth Amendment. *See Klayman v. Obama*, 2013 U.S. Dist. LEXIS 176925 and *ACLU v. Clapper*, 2013 U.S. Dist. LEXIS 180863. Thus, Petitioners file under the authority of Title 28, U.S.C. Section 2101(e) and Rule 11 of the Supreme Court. The district court granted Petitioner's motion for preliminary injunction on December 16, 2013 and stayed the order pending appeal. Respondent filed a notice of appeal on January 3, 2014, in the U.S. Court of Appeals for the District of Columbia Circuit (hereinafter D.C. Circuit) and that court has not issued a final order. Thus no final judgment has been issued and the case can and must, respectfully, for the compelling reasons set forth below, be directly reviewed by the Supreme Court under 28 U.S.C. § 2101(c).

OPINION BELOW

The opinion of the district court granting Petitioners' motion for preliminary injunction as to Larry Klayman and Charles Strange is reported as *Klayman v. Obama*, Civil Action No. 13-851 (*Klayman I*). The opinion is also available at 2013 U.S. Dist. LEXIS 176925.

JURISDICTION

The preliminary injunction order of the district court was entered on December 16, 2013. The jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1), 28 U.S.C. § 2101, and Rule 11 of the Supreme Court. Pursuant to 28 U.S.C. § 1254(1), this Court may grant a petition for a writ of certiorari to review any case that is pending in the court of appeals if a final judgment has not been entered by that court. *United States v. Nixon,* 418 U.S. 683, 692 (1974).

CONSTITUTIONAL AND STATUTORY PROVISIONS

1. The Fourth Amendment to the U.S. Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against

unreasonable searches and seizures."[3] U.S. CONST. amend. IV.

STATEMENT OF THE CASE

Petitioners request the Supreme Court to exercise its power and discretion under Rule 11 to grant a writ of certiorari before judgment to the D.C. Circuit, which has not yet entered judgment on an appeal of this case pending before it.

I. PROCEDURAL HISTORY.

The original complaint in the proceeding below was filed on June 6, 2013 and the amended complaint was filed on June 9, 2013. Thereafter, Petitioners filed a motion for preliminary injunction on October 29, 2013. The NSA Respondents, through the U.S. Justice Department, responded on November 12, 2013. The district court then held an oral argument on November 18, 2013. At oral argument, the district court ordered any supplemental briefs to be filed on or before November 26, 2013. Both Petitioners and NSA Respondents filed the supplemental briefs on November 26, 2013. On December 16, 2013, the district court issued a preliminary injunction against

[3] The subject preliminary injunction order did not address or reach Petitioners' First and Fifth Amendment claims.

the NSA and other Government Defendants, but stayed its order pending appeal. In doing so, the district court admonished the NSA and the other Government Defendants, directing them to move through the appellate process quickly. Specifically, Judge Leon stayed the order but expected that the appellate courts and Supreme Court would address the violations of Fourth Amendment rights expeditiously, as these egregious violations would undoubtedly be continuing. He ruled: "I fully expect . . . the Government will take whatever steps necessary to prepare itself to comply with this order when, and if, it is upheld. Suffice it to say, requesting further time to comply with this order months from now will not be well received and could result in collateral sanctions." App. 89. However, on January 3, 2014, almost three (3) weeks after the district court's order granting a preliminary injunction, in an obvious effect to delay adjudication of its appeal, the NSA Respondents filed its notice of appeal before the D.C. Circuit. A simple notice of appeal could have been filed on the same day that Judge Leon issued his order, December 16, 2013. The D.C. Circuit then issued its scheduling order on January 13, 2014.

II. FACTUAL BACKGROUND.

Congress passed the Foreign Intelligence Surveillance Act (FISA) in 1978 to prevent the indiscriminate and invasive domestic surveillance of Americans

by Government intelligence agencies. *See* S. Rep. No. 95-604(I) at 7 (1977), reprinted in 1978 U.S.C.C.A.N. 3904, 3908 ("This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused."); David S. Kris & J. Douglas Wilson, National Security Investigations & Prosecutions §§ 2.2-2.6, 3.4 (2d ed. 2012) (discussing a "history of abuse" within the Intelligence Community) (hereinafter "Kris & Wilson"). The FISA required the Government to limit surveillance to specific, targeted investigations of foreign agents and foreign powers, and consequently it created the FISC to oversee and authorize such surveillance. As Justice Samuel Alito recently stated for the Court in *Clapper*:

> Congress enacted the Foreign Intelligence Surveillance Act (FISA) to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes. See 92 Stat. 1783, 50 U.S.C. § 1801 et seq.; D. Kris & J. Wilson, National Security Investigations & Prosecutions §§ 3.1, 3.7 (2d ed. 2012) (Kris & Wilson).
>
> [. . .]
>
> In FISA, Congress authorized judges of the Foreign Intelligence Surveillance Court (FISC) to approve electronic surveillance for foreign intelligence purposes if there is probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power," and that each of

> the specific "facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." § 105(a)(3), 92 Stat. 1790; see § 105(b)(1)(A), (b)(1)(B), *ibid.*; 1 Kris & Wilson § 7:2, at 194-195; *id.*, § 16:2, at 528-529.

Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).

Under 50 U.S.C. § 1861, the Federal Bureau of Investigation (FBI) may apply for a FISC order to compel the production of "tangible things," typically from a business. 50 U.S.C. § 1861(a)(1). However, the application must show that there are "reasonable grounds" to believe the tangible things sought are relevant to an authorized investigation and the investigation must "be conducted under guidelines approved by the Attorney General under Executive Order 12,333." 50 U.S.C. § 1861(a)(2)(A). If, and only if, the FISC finds that the FBI's application meets the statutory requirements, then the FISC "shall enter an ex parte order as requested, or as modified, approving the release of tangible things." 50 U.S.C. § 1861(c)(1).

In enacting FISA to regulate government surveillance conducted for foreign-intelligence purposes, Congress also created the FISC and empowered it to grant or deny Government applications for surveillance orders in foreign-intelligence investigations. *See* 50 U.S.C. § 1803(a). Over time, several acts and successor bills, including the Patriot Act, modified the

provisions provided under FISA in several respects. In its current form, the Patriot Act (now referred to as Section 215) allows the Government to obtain an order compelling production of "any tangible things" *only if* the government "show[s] that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(b)(2)(A). Section 215, even if constitutional, does not provide the Government with limitless investigative power. Rather, the language added by the Patriot Act prohibits the government from using the statute to obtain things that could not be obtained through analogous mechanisms, such as a subpoena duces tecum. 50 U.S.C. § 1861(c)(2)(D). Until recently, the public knew little about the NSA Respondents' abuse of the statute to unlawfully obtain detailed intimate information regarding ordinary Americans not connected to terrorists or terrorism, in violation of the U.S. Constitution and fundamental rights against unreasonable searches and seizures.[4]

---

[4] President Obama effectively admitted the unlawful acts of his NSA Respondents during a recent speech where he suggested reforms to the Government's surveillance of all American citizens. He stated, "I believe we need a new approach." In doing so, President Obama rebuked Judge Pauley's and the FISC's interpretation of the law as they found the NSA Respondents' conduct to be lawful. However, the president's recommendations

(Continued on following page)

The NSA Respondents' absolute disregard of, if not contempt for, the limitations set forth in Section 215 have been evidenced through numerous instances of unlawful conduct, including repeatedly misleading the FISC, presenting inaccurate statements in court filings, making outright false statements, and exceeding the bounds of the surveillance orders, as further detailed below. *See* Judge Bates' Mem. Op., *In re Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certification* (FISC Ct. Oct. 3, 2013); *See also*, Nicole Perlott, Jeff Larson, and Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web,* The N.Y. Times (Sept. 5, 2013), http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html.

The misleading statements made by senior officials regarding the domestic surveillance program and the egregious extent of the NSA Respondents' false misrepresentations constitute perjury. For instance, the National Intelligence Director, James Clapper, testified before Congress earlier this year that the NSA Respondents do not collect *any* type of data on hundreds of millions of Americans, which he was forced to later admit once he was exposed to have

---

are unlikely to rectify the ongoing lawlessness; only this Court can rectify the lawlessness by settling its constitutional issues among its lower courts.

lied, is a "clearly erroneous" lie. Sen. Ron Wyden asked Clapper during a hearing in March of 2013 if the NSA Respondents gathered "any type at all on millions or hundreds of millions of Americans."[5] Clapper initially answered definitively: "No." When pressed by Wyden, Clapper changed his answer. "Not wittingly," he said. "There are cases where they could inadvertently perhaps collect, but not wittingly." Nothing could be further from the truth, as evidenced by Clapper's subsequent apology for his clearly erroneous and perjurious answer and the public disclosure of a highly classified secret Verizon Order.

In March 2009, the FISC learned that the NSA Respondents' analysts used the phone log database in ways beyond what the judges believed to be legal because of the NSA Respondents' repeated false statements in court filings. In 2011, a federal judge, John D. Bates, then serving as Chief Judge of the FISC, issued an 85-page ruling, which sharply rebuked the NSA Respondents for repeatedly misleading the court that oversees its surveillance on domestic soil, including a program that is collecting tens of thousands of domestic e-mails and other Internet communications of Americans each year. Mem. Op., *In re Government's Ex Parte Submission of Reauthorization Certification and Related Procedures,*

---

[5] *See Clapper apologizes for 'erroneous' answer on NSA*, http://news.yahoo.com/clapper-apologizes-erroneous-answer-nsa-221238030.html (summarizing Clapper's misleading statements to Congress on the extent of U.S. surveillance on U.S. citizens).

Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certification (FISC Ct. Oct. 3, 2013). Judge Bates further admonished the NSA Respondents for repeatedly violating the requirements and limitations set forth by court orders, privacy laws, and the U.S. Constitution, recognizing that, "[c]ontrary to the government's repeated assurances, N.S.A. has been routinely running queries of the metadata using querying terms that did not meet the standard for querying," and that this requirement had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively." *Id.*; *see also*, Charlie Savage and Scott Shane, *Secret Court Rebuked N.S.A. on Surveillance,* N.Y. Times, Aug. 21, 2013. Judge Bates further emphasized the NSA's unlawful conduct and egregious and illicit surveillance tactics, by stating:

> The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program. In March, 2009, the Court concluded that its authorization of NSA's bulk acquisition of telephone call detail records from [redacted] in the so-called "big business records" matter "ha[d] been premised on a flawed depiction of how the NSA uses [the acquired] metadata," and that

> "[t]his misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions . . .

Mem. Op., *In re Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certification* (FISC Ct. Oct. 3, 2013) at n. 14.

The NSA Respondents have continuously engaged in a pattern of non-compliance with respect to the NSA Respondents' handling of produced information, as demonstrated through publicly released FISC orders addressing the NSA's surveillance and requests for production of information. In her Amended Memorandum Opinion dated August 29, 2013, the Honorable Claire V. Eagan recognized and acknowledged the NSA Respondents' repeated lack of adherence to minimization procedures implicit in the authorization to compel production of the documents. Judge Eagan stated, "[t]he Court is aware that in prior years there have been incidents of non-compliance with respect to NSA's handling of produced information." Am. Mem. Op., *In Re Application of the [FBI] for an Order Requiring the Production of Tangible Things From [Redacted]* (FISC Ct. Aug. 29, 2013) at n. 9.

Similarly, in an order issued by the FISC on March 2, 2013, questioning the credibility, trustworthiness, and ability of the NSA Respondents to fully comply with court orders, the Honorable Reggie B. Walton held:

> "[i]n light of the scale of this bulk [telephone records] collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified . . . and that it is being implemented in a manner that protects the privacy interests of U.S. persons as required by applicable minimization procedures. To approve such a program, the Court must have every confidence that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders. ***The Court no longer has such confidence.***"

(Emphasis added) *In Re Production of Tangible Things [Redacted]*, Dkt. No. BR. 08-13 (FISA Ct. March 2, 2009).

Alarmingly, it has recently been discovered that even lower level officials have been willfully and intentionally misusing the NSA Respondents' surveillance power to spy on their paramours. The NSA Inspector General George Ellard admitted that since 2003, there have been " . . . substantiated instances of intentional misuse" of "surveillance authorities." About all of these cases involved an NSA employee spying on a girlfriend, boyfriend, or some kind of love

interest. Jake Gibson, *Too tempting? NSA watchdog details how officials spied on love interests,* FOX News (Sept. 27, 2013), http://www.foxnews.com/politics/2013/09/27/too-tempting-nsa-details-how-officials-spied-on-love-interests. More concerning, if lower level employees are capable of such misuse of the agency's surveillance power, then imagine what the higher officials, who play at the upper levels of Government and politics are capable of with access to such surveillance programs.[6]

REASONS FOR GRANTING THE PETITION

As provided in 28 U.S.C. § 1254(1), cases in the court of appeals may be reviewed by the Supreme Court "by writ of certiorari granted upon the petition of any party to any civil or criminal case, before or after rendition of judgment or decree." 28 U.S.C. § 2101. Section 2101 further provides that "an application to the Supreme Court for a writ of certiorari to

[6] Notably, further evidencing the agency's surveillance power and its misuse is the fact that the NSA even went so far as to monitor the phone calls of 35 world leaders, including Germany's Chancellor Angela Merkel's phone, which has led to the "worst spat between the two countries in a decade." Reuters, *NSA Monitored Phone Calls of 35 World Leaders*, The Huffington Post, Oct. 24, 2013, http://www.huffingtonpost.com/2013/10/24/nsa-world-leaders_n_4158922.html. Such surveillance has also involved France, Mexico, and Brazil, as well as other countries. *Report says NSA monitored 35 world leaders, on heel of Merkel spying claim,* FOX News (Oct. 25, 2013).

review a case before judgment has been rendered in the court of appeals may be made at any time before judgment." Pursuant to Rule 11 of the Supreme Court, "a petition for writ of certiorari to review a case pending in a United States court of appeals, before judgment is entered in that court, will be granted if there is a showing that the case is of such imperative public importance as to justify deviation from normal appellate practice and to require immediate determination in this Court." Sup. Ct. R. 11. This is that sort of case.

I. THIS CASE IS OF IMPERATIVE NATIONAL IMPORTANCE REQUIRING IMMEDIATE DETERMINATION IN THIS COURT.

Early on in this case, the Honorable Richard J. Leon, whose preliminary injunction order is on appeal, remarked about the importance of the constitutional issues now before this Court, and why expeditious adjudication and determination is imperative. Specifically, Judge Leon emphasized to the NSA Respondents:

> We work 24/7 around this courthouse, my friend. 24/7. I don't want to hear anything about vacations, weddings, days off. Forget about it. This is a case at the pinnacle of public national interest, pinnacle. All hands 24/7. No excuses. You got a team of lawyers. Mr. Klayman is alone apparently. You [the U.S. Justice Department] have litigated cases in this courthouse when it is matters of

> this consequence and enormity. You know how this Court operates.[7]

Transcript of Status Conference of October 31, 2013 at pg. 7 (Tr. of St. Conf.). In later issuing the subject preliminary injunction order of December 16, 2013, Judge Leon held with regard to the severity of the constitutional law violations being perpetrated on nearly the entire U.S. citizenry: "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every single citizen for the purposes of querying it and analyzing it without judicial approval." App. 84. He continued:

> No court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion . . . I have little doubt that the author of the Constitution, James Madison, who cautioned us to beware 'the abridgement of freedom of the

[7] Despite the Court's order granting a preliminary injunction on December 16, 2013, the NSA Respondents did not file a notice of appeal until almost three (3) weeks later on January 3, 2014. A simple notice of appeal could have been filed forthwith consistent with the district court's direction to accelerate any appeals given Judge Leon's deference to them in staying the preliminary injunction order. As set forth below, this intentional delay is consistent with the NSA Respondents' and the Obama Justice Department's strategic goal to delay adjudication of these cases and to flout court orders.

> people by gradual and silent encroachments by those in power,' would be aghast.[ ]

App. 84, 85.

Indeed, Judge Leon ruled that this case is of national public importance: "[The public] interest looms large in this case, given the significant privacy interests at stake and the unprecedented scope of the NSA's collection and querying efforts, which likely violate the Fourth Amendment." App. 86.

Following the issuance of Judge Leon's preliminary injunction order, legal scholars, both liberal and conservative such as Laurence Tribe of Harvard Law School and Randy Barnett of Georgetown Law School, opined that the ultimate adjudication of the constitutional issues would ultimately have to go before this Court. This was even before the Honorable William H. Pauley III of the U.S. District Court for the Southern District of New York issued an order on December 27, 2013 dismissing a similar case filed by the American Civil Liberties Union (ACLU). *ACLU v. Clapper*, 2013 U.S. Dist. LEXIS 180863.

Incredibly, Judge Pauley's decision is diametrically at odds with the preliminary injunction order of Judge Leon. Putting the so-called right to, in effect, indiscriminately and massively spy on American citizens with no connection to terrorists or terrorism ahead of civil liberties and privacy, Judge Pauley found: "This blunt tool only works because it collects everything . . . such data can reveal a rich profile of

every individual as well as a comprehensive record of people's associations with one another." Judge Pauley's Memorandum Opinion of December 27, 2013 at pg. 2 (App. 91). Judge Pauley continued, " . . . the Government acknowledged that since May 2006, it has collected [telephony metadata] for substantially every telephone call in the United States, including calls between the United States and a foreign country and calls entirely within the United States." App. 101. Yet Judge Pauley's conclusion is most telling and indeed frightening: "The right to be free from searches and seizures is fundamental, but not absolute . . . " App. 155, and "[t]he choice between liberty and security is a false one . . . " App. 157. Contrary to Judge Pauley's reasoning, one does not have to make a choice between liberty and security as the two are not mutually exclusive under the U.S. Constitution. As former Vice President, U.S. Senator, and 2000 presidential candidate Al Gore warns, "[s]urveillance technologies now available – including the monitoring of virtually all digital information – have advanced to the point where much of the essential apparatus of a police state is already in place." Suzanne Goldenberg, *Al Gore: NSA's secret surveillance program 'not really the American way'*, The Guardian (June 14, 2013, 15.49 EDT), http://www.theguardian.com/world/2013/jun/14/al-gore-nsa-surveillance-unamerican.

Following Judge Pauley's decision, only about a week or so later, another Article III court further

muddied and obfuscated the constitutional waters of the NSA Respondents' massive scheme to spy on the American citizenry by collecting and accessing the telephonic metadata of even those who are not under investigation and have no connection to terrorists or terrorism. Defiantly seeking to justify its having rubberstamped in secret chamber proceedings the illegal actions of the NSA Respondents in the past, despite their repeated lying about the NSA's activities, the FISC approved another ninety (90) days of this blanket, indiscriminate surveillance – arrogantly flouting the ruling of Judge Leon. Incredibly, the FISC, by the urging of Director of Intelligence James Clapper, also subsequently and publicly released a letter to Senator Diane Feinstein, Chairman of the Select Committee on Intelligence, seeking to undercut proposals to reign in the NSA Respondents' illegality by allowing some very limited and still secretive public advocacy before the FISC on behalf of third parties subject to surveillance. Apparently, the FISC believes that it should continue to have unbridled powers to do in secret as it pleases and that ordinary innocent Americans should have no right to challenge its actions, let alone even know what it orders. http://www.pbs.org/newshour/rundown/2014/01/fisa-court-reauthorizes-nsa-phone-surveillance-program.html.

In effect, this grave constitutional violation of Fourth Amendment rights has caused a virtual legal war among the judiciary – a war that can only be resolved by this Court. Not only are there huge constitutional issues at bar, but the division among

these dueling Article III courts also cries out for immediate intervention as the Fourth Amendment rights of American citizens continue to be violated in an "almost-Orwellian" fashion.

Thus, it is no wonder that there is nearly unanimous consensus among legal experts and others that this Court must grant a writ of certiorari and break the impasse among these Article III courts. And, the issues presented here are far more important than the issues presented in earlier successful writs, where this Court took immediate jurisdiction under Rule 11. These cases include but are not limited to challenges to the legality of the Federal Sentencing Guidelines in *Mistretta v. United States*, 488 U.S. 361 (1989), the reorganization of two railroads in *New Haven Inclusion Cases*, 399 U.S. 392, 418 (1970), a coal strike in *United States v. Mineworkers of America*, 330 U.S. 258, 269 (1947), and a denial of the power of a federal court to enforce rent control in *Porter v. Dicken*, 328 U.S. 252 (1946).

Rule 11 thus has been used in a wide range of circumstances. *Gratz v. Bollinger*, 539 U.S. 244, 259-60 (2003). But none have been so compelling as in this instance, where in the words of a well respected federal judge, Richard J. Leon, the NSA's massive collection and use of metadata has, in an "almost-Orwellian" fashion, resulted in the government spying and violating the Fourth Amendment rights of nearly the entire U.S. citizenry, notwithstanding the Petitioners below. This is potentially the greatest ongoing violation of constitutional rights in American

history, amounting to what in effect has become, as former Vice President Al Gore puts it, a police state. And, indeed, it is black letter law that this continuing legal outrage cannot and should not continue for one minute more than it takes this Court to break the legal impasse and settle the constitutional issues and split among the courts at bar. *Mills v. District of Columbia*, 571 F.3d 1304, 1312 (D.C. Cir. 2009) (quoting *Elrod v. Burns*, 427 U.S. 347, 373 (1976) (plurality opinion)).

II. THE IMPERATIVE PUBLIC IMPORTANCE OF THE CONSTITUTIONALITY OF THE DEFENDANTS' ACTIONS JUSTIFY DEVIATION FROM NORMAL APPELLATE PRACTICE.

As set forth above, the imperative public importance of this case cries out for deviation from normal appellate practice, as time is of the essence in having this Court decide what are the constitutional Fourth Amendment rights to protect the nearly 300 million Americans who continue to be indiscriminately spied upon by the NSA and who are not under investigation for ties to terrorists or terrorism. Judge Leon states, " . . . [the public] interest looms large[ ] in this case, given the significant privacy interests at stake and the unprecedented scope of the NSA's collection and querying efforts, which likely violate the Fourth Amendment." This Court must address this "almost-Orwellian" violation of Fourth Amendment rights and not allow this outrageous intrusion

of privacy to continue for any longer than necessary. As *Mills* holds, **" . . . the loss of constitutional freedoms, 'for even minimal periods of time, unquestionably constitutes irreparable injury.'"** *Mills,* 571 F.3d 1304 at 1312. Early and immediate review by writ of certiorari by this Court is imperative to address as soon as practicable the continuing Fourth Amendment violations that are causing irreparable injury to Petitioners and the American people as a whole on a minute-by-minute basis. The American people have a right to expect no less from their judiciary and this Court, which was designed by our Founding Fathers to serve as a check on the tyranny of the other two branches of government, and thus head off another revolution.

III. THIS CASE IS PROPER FOR CERTIFICATION AND IS THE ONLY VEHICLE FOR RESOLVING CONSTITUTIONAL ISSUES WHICH HAVE BEEN VARIOUSLY DECIDED AROUND THE COUNTRY AND WHICH CAN ONLY BE FINALLY DECIDED IN THIS COURT.

This Court can resolve the constitutional split between three Article III courts and must do so at the earliest opportunity. *Id*. This Court has deemed a split among district courts in different circuits as a factor weighing in favor of granting certiorari under Rule 11. *Mistretta v. United States*, 488 U.S. 361, 371 (1989). Such a split exists here and has merely been deepened by the opposite New York decision and the

recent defiant FISC decision. *See ACLU v. Clapper*, 2013 U.S. Dist. LEXIS 180863. Granting the writ of certiorari is the only vehicle for resolving the split so the Fourth Amendment rights of Petitioners and all Americans are resolved expeditiously as this gross violation of the U.S. Constitution is continuing.

The fact that Petitioners were the prevailing party below is no barrier to the grant of certiorari. 28 U.S.C. § 1254(1) provides that "any party to any civil or criminal case" may petition for certiorari from "[c]ases in the courts of appeals" both "before and after rendition of judgment or decree." 28 U.S.C. § 1254(1).

CONCLUSION

For the foregoing reasons, the petition for writ of certiorari before judgment in the D.C. Circuit should be granted. This amounts to perhaps the most egregious widespread violation of constitutional rights of the American people in U.S. history. Respectfully, this Court must address and resolve these constitutional issues at the earliest practicable date before further harm is done to the hundreds of millions of Americans

who have no connection to terrorists or terrorism, and who now, in the words of Thomas Jefferson, have been made to fear their Government.

Dated: February 3, 2014

Respectfully submitted,

LARRY KLAYMAN, ESQ.
2020 Pennsylvania Ave. NW, #345
Washington, DC 20006
Tel: (310) 595-0800
Email: leklayman@gmail.com

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KLAYMAN et al.,	
Plaintiffs,	
v.	**Civil Action No. 13-0851 (RJL)**
OBAMA et al.,	
Defendants.	
KLAYMAN et al.,	
Plaintiffs,	
v.	
OBAMA et al.,	
Defendants.	

ORDER

(Filed Dec. 16, 2013)

For the reasons set forth in the Memorandum Opinion entered this date, it is this 16th day of December, 2013, hereby

ORDERED that the Motion for Preliminary Injunction in *Klayman v. Obama,* Civil Action No. 13-0851 (*Klayman 1*) [Dkt. # 13], is **GRANTED** as to plaintiffs Larry Klayman and Charles Strange and **DENIED** as to plaintiff Mary Ann Strange; it is further

ORDERED that the Government:

(1) is barred from collecting, as part of the NSA's Bulk Telephony Metadata Program, any telephony metadata associated with Larry Klayman's and Charles Strange's personal Verizon telephone subscriptions; and

(2) must destroy all such metadata already collected under the Bulk Telephony Metadata Program; it is further

ORDERED that the Motion for Preliminary Injunction in *Klayman v. Obama,* Civil Action No. 13-0881 (*Klayman II*) [Dkt. # 10] is **DENIED**; and it is further

ORDERED that this Order is **STAYED** pending appeal.

/s/ Richard J. Leon
RICHARD J. LEON
United States District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

KLAYMAN et al.,	
Plaintiffs,	
v.	**Civil Action No. 13-0851 (RJL)**
OBAMA et al.,	
Defendants.	
KLAYMAN et al.,	
Plaintiffs,	
v.	
OBAMA et al.,	
Defendants.	

MEMORANDUM OPINION
December 16, 2013 [Dkt. # 13 (No. 13-0851), # 10 (No. 13-0881)]

(Filed Dec. 16, 2013)

On June 6, 2013, plaintiffs brought the first of two related lawsuits challenging the constitutionality and statutory authorization of certain intelligence-gathering practices by the United States government relating to the wholesale collection of the phone

record metadata of all U.S. citizens.[1] These related cases are two of several lawsuits[2] arising from public revelations over the past six months that the federal government, through the National Security Agency ("NSA"), and with the participation of certain telecommunications and internet companies, has conducted surveillance and intelligence-gathering programs that collect certain data about the telephone and internet activity of American citizens within the United States. Plaintiffs – five individuals in total between No. 13-851 ("*Klayman I*") and No. 13-881 ("*Klayman II*") – bring these suits as U.S. citizens who are subscribers or users of certain telecommunications and internet firms. *See* Second Am. Compl. (*Klayman I*) [Dkt. # 37] ¶ 1; Am. Compl. (*Klayman II*) [Dkt. # 30] ¶ 1.[3] They bring suit against both federal government

---

[1] Plaintiffs' second suit was filed less than a week later on June 12, 2013, and challenged the constitutionality and statutory authorization of the government's collection of both phone and internet metadata records.

[2] The complaint in *ACLU v. Clapper,* Civ. No. 13-3994, which was filed in the United States District Court for the Southern District of New York on June 11, 2013, alleges claims similar to those in the instant two cases. *See also In re Electronic Privacy Information Center,* No. 13-58 (S. Ct.) (Petition for a Writ of Mandamus and Prohibition, or a Writ of Certiorari filed July 8, 2013; petition denied Nov. 18, 2013); *Smith v. Obama,* Civ. No. 2:13-00257 (D. Idaho) (complaint filed June 12, 2013); *First Unitarian Church of Los Angeles v. NSA,* Civ. No. 13-3287 (N.D. Cal.) (complaint filed July 16, 2013).

[3] Plaintiffs' complaints reflect their intention to bring both suits as class actions on behalf of themselves and "all other similarly situated consumers, users, and U.S. citizens who are

(Continued on following page)

defendants (several federal agencies and individual executive officials) and private defendants (telecommunications and internet firms and their executive officers), alleging statutory and constitutional violations. *See generally* Second Am. Compl. (*Klayman I*); Am. Compl. (*Klayman II*).

Before the Court are plaintiffs' two Motions for Preliminary Injunction [Dkt. # 13 (*Klayman I*), # 10 (*Klayman II*)], one in each case. As relief, plaintiffs seek an injunction "that, during the pendency of this suit, (i) bars [d]efendants from collecting [p]laintiffs' call records under the mass call surveillance program; (ii) requires [d]efendants to destroy all of [p]laintiffs' call records already collected under the program; and (iii) prohibits [d]efendants from querying metadata obtained through the program using any phone number or other identifier associated with [p]laintiffs . . . and such other relief as may be found just and proper." Pls.' Mot. for Prelim. Inj. (*Klayman I*) [Dkt. # 13]; Pls.' Mot. for Prelim. Inj. (*Klayman II*) [Dkt. # 10]; *see also* Pls.' Mem. P. & A. in Supp. of Mot. for Prelim. Inj.

---

customers and users of," Second Am. Compl. ("*Klayman I*") ¶ 1, or "who are subscribers, users, customers, and otherwise avail themselves to," Am. Compl. ("*Klayman II*") 11, the telecommunications and internet companies named in the complaints. Plaintiffs have not yet, however, moved to certify a class in either case and in fact have moved for extensions of time to file a motion for class certification four times in each case. *See* Motion for Extension of Time to Certify Class Action (*Klayman I*) [Dkt. # # 7, 14, 27, 40]; (*Klayman II*) [Dkt. # # 6, 11, 23, 33].

(*Klayman I*) ("Pls.' Mem.") [Dkt. # 13-1], at 30-31.[4] In light of how plaintiffs have crafted their requested relief, the Court construes the motions as requesting a preliminary injunction (1) only as against the federal government defendants, and (2) only with regard to the government's bulk collection and querying of phone record metadata. Further, between the two cases, plaintiffs have alleged with sufficient particularity that only two of the five named plaintiffs, Larry Klayman and Charles Strange, are telephone service subscribers.[5] Accordingly, for purposes of resolving

---

[4] Unless otherwise indicated, all citations to "Pls.' Mem." and other docket items hereinafter shall refer to the filings made in *Klayman I*.

[5] In *Klayman I,* plaintiffs Larry Klayman and Charles Strange have submitted affidavits stating they are subscribers of Verizon Wireless for cellular phone service, *see* Aff. of Larry Klayman ("Klayman Aff.") [Dkt. # 13-2], at ¶ 3; Suppl. Aff. of Larry Klayman ("Klayman Suppl. Aff.") [Dkt. # 31-2], at ¶ 3; Aff. of Charles Strange ("Strange Aff.") [Dkt. # 13-3], at ¶ 2, but neither the complaint nor the motion affirmatively alleges that Mary Ann Strange is a subscriber of Verizon Wireless or any other phone service, *see* Second Am. Compl. ¶ 10 (describing plaintiff Mary Ann Strange). And in *Klayman II,* where the complaint and motion raise claims regarding the government's collection and analysis of both phone and internet records, the plaintiffs neither specifically allege, nor submit any affidavits stating, that any of them individually is a subscriber of either of the two named telephone company defendants, AT&T and Sprint, *for telephone services. See* Aff. of Larry Klayman (*Klayman II*) [Dkt. # 10-2], at ¶ 3 ("I am also a user of internet services by . . . AT & T. . . ."); Suppl. Aff. of Larry Klayman (*Klayman II*) [Dkt. # 26-2], at ¶ 3 (same); Aff. of Charles Strange (*Klayman II*) [Dkt. # 10-3], at ¶ 3 ("I am also a user of internet services by . . . AT&T. . . ."); Am. Compl. ¶ 14 ("Plaintiff Garrison

(Continued on following page)

these two motions, the Court's discussion of relevant facts, statutory background, and legal issues will be circumscribed to those defendants (hereinafter "the Government"), those two plaintiffs (hereinafter "plaintiffs"), and those claims.[6]

. . . is a consumer and user of Facebook, Google, YouTube, and Microsoft products."). *Compare* Am. Compl. (*Klayman II*) ¶ 13 ("Plaintiff Ferrari . . . is a subscriber, consumer, and user of *Sprint,* Google/Gmail, Yahoo!, and Apple. As a prominent private investigator, Ferrari regularly communicates, both telephonically and electronically. . . ." (emphasis added)), *with* Pls.' Mem. (*Klayman II*) [Dkt. # 10-1], at 18 ("Defendants have indisputably also provided the NSA with intrusive and warrantless access to the *internet records* of Plaintiffs Michael Ferrari and Matthew Garrison" (emphasis added)).

[6] *Klayman I* concerns only the collection and analysis of phone record data, and only with respect to private defendant Verizon Communications. *Klayman II,* by contrast, appears to concern the collection and analysis of both phone and internet record data, and includes both phone companies and internet companies as private defendants. In the latter case, Plaintiffs' Motion for Preliminary Injunction [Dkt. # 10] and their Memorandum of Points and Authorities in Support [Dkt. # 10-1] suffer from some confusion as a result of its larger scope. On the face of the Motion itself [Dkt. # 10] and their Proposed Order [Dkt. # 10-4], plaintiffs request relief that is identical to that requested in the motion in *Klayman I* – i.e., relief concerning only the collection and querying of phone record data. Throughout the memorandum in support [Dkt. # 10-1], however, plaintiffs intermingle claims regarding the surveillance of phone and internet data, and then in conclusion request relief arguably concerning only internet data. *See* Pls.' Mem. P. & A. Supp. Mot. Prelim. Inj. (*Klayman II*) [Dkt. # 10-1], at 4, 32 (requesting an injunction that, in part, "bar[s] Defendants from collecting records pertaining to Plaintiffs' online communications and internet activities").

(Continued on following page)

For the reasons discussed below, the Court first finds that it lacks jurisdiction to hear plaintiffs' Administrative Procedure Act ("APA") claim that the Government has exceeded its statutory authority

---

To the extent plaintiffs are, in fact, requesting preliminary injunctive relief regarding any alleged internet data surveillance activity, the Court need not address those claims for two reasons. First, the Government has represented that any bulk collection of internet *metadata* pursuant to Section 215 (50 U.S.C. § 1861) was discontinued in 2011, *see* Govt. Defs.' Opp'n to Pls.' Mot. for Prelim. Inj. ("Govt.'s Opp'n") [Dkt. # 25], at 15-16, 44-45; Ex. J to Decl. of James J. Gilligan ("Gilligan Deck") [Dkt. # 25-11] (Letter from James R. Clapper to the Sen. Ron Wyden (July 25, 2013)), and therefore there is no possible ongoing harm that could be remedied by injunctive relief. Second, to the extent plaintiffs challenge the Government's targeted collection of internet data *content* pursuant to Section 702 (50 U.S.C. § 1881a) under the so-called "PRISM" program, which targets non-U.S. persons located outside the U.S., plaintiffs have not alleged sufficient facts to show that the NSA has targeted any of their communications. *See* Govt.'s Opp'n at 21-22, 44. Accordingly, plaintiffs lack standing, as squarely dictated by the Supreme Court's recent decision in *Clapper v. Amnesty International USA,* 133 S. Ct. 1138 (2013), which concerns the same statutory provision. In *Clapper,* the Court held that respondents, whose work purportedly involved engaging in phone and internet contact with persons located abroad, lacked standing to challenge Section 702 because it was speculative whether the government would seek to target, target, and actually acquire their communications. *See Clapper,* 133. S. Ct. at 1148-50 ("[R]espondents' speculative chain of possibilities does not establish that injury based on potential future surveillance is certainly impending or is fairly traceable to § 1881a."). So too for plaintiffs here. (In fact, plaintiffs here have not even alleged that they communicate with anyone outside the United States at all, so their claims under Section 702 are even less colorable than those of the plaintiffs in *Clapper*.)

under the Foreign Intelligence Surveillance Act ("FISA"). Next, the Court finds that it does, however, have the authority to evaluate plaintiffs' constitutional challenges to the NSA's conduct, notwithstanding the fact that it was done pursuant to orders issued by the Foreign Intelligence Surveillance Court ("FISC"). And after careful consideration of the parties' pleadings and supplemental pleadings, the representations made on the record at the November 18, 2013 hearing regarding these two motions, and the applicable law, the Court concludes that plaintiffs have standing to challenge the constitutionality of the Government's bulk collection and querying of phone record metadata, that they have demonstrated a substantial likelihood of success on the merits of their Fourth Amendment claim, and that they will suffer irreparable harm absent preliminary injunctive relief.[7] Accordingly, the Court will GRANT, in part, the

[7] Because I ultimately find that plaintiffs have made a sufficient showing to merit injunctive relief on their Fourth Amendment claim, I do not reach their other constitutional claims under the First and Fifth Amendments. *See Seven-Sky v. Holder,* 661 F.3d 1, 46 (D.C. Cir. 2011) (noting "the bedrock principle of judicial restraint that courts avoid prematurely or unnecessarily deciding constitutional questions"), *abrogated by Nat'l Fed'n of Indep. Bus. v. Sebelius,* 132 S. Ct. 2566 (2012); *see also Wash. State Grange v. Wash. State Republican Party,* 552 U.S. 442, 450 (2008) (noting "the fundamental principle of judicial restraint that courts should neither anticipate a question of constitutional law in advance of the necessity of deciding it nor formulate a rule of constitutional law broader than is required by the precise facts to which it is to be applied" (citations and internal quotation marks omitted)).

Motion for Preliminary Injunction in *Klayman I* (with respect to Larry Klayman and Charles Strange only), and DENY the Motion for Preliminary Injunction in *Klayman II*. However, in view of the significant national security interests at stake in this case and the novelty of the constitutional issues, I will STAY my order pending appeal.

BACKGROUND

On June 5, 2013, the British newspaper *The Guardian* reported the first of several "leaks" of classified material from Edward Snowden, a former NSA contract employee, which have revealed – and continue to reveal – multiple U.S. government intelligence collection and surveillance programs. *See* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily,* GUARDIAN (London), June 5, 2013.[8] That initial media report disclosed a FISC order dated April 25, 2013, compelling Verizon Business Network Services to produce to the NSA on "an ongoing daily basis . . . all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." Secondary Order, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from Verizon Business Network*

[8] *Available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Services, Inc. on Behalf of MCI Communication Services, Inc. d/b/a Verizon Business Services, No. BR 13-80 at 2 (FISC Apr. 25, 2013) (attached as Ex. F to Gilligan Decl.) [Dkt. # 25-7] ("Apr. 25, 2013 Secondary Order"). According to the news article, this order "show[ed] . . . that under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk – regardless of whether they are suspected of any wrongdoing." Greenwald, *supra.* In response to this disclosure, the Government confirmed the authenticity of the April 25, 2013 FISC Order, and, in this litigation and in certain public statements, acknowledged the existence of a "program" under which "the FBI obtains orders from the FISC pursuant to Section 215 [of the USA PATRIOT Act] directing certain telecommunications service providers to produce to the NSA on a daily basis electronic copies of 'call detail records.'" Govt's Opp'n at 8.[9] Follow-on media reports

[9] Although aspects of the program remain classified, including which other telecommunications service providers besides Verizon Business Network Services are involved, the Government has declassified and made available to the public certain facts about the program. *See* Office of the Dir. of Nat'l Intelligence, *DNI Statement on Recent Unauthorized Disclosure of Classified Information* (June 6, 2013), *available at* http://www.dni.gov/index.php/newsroom/pressreleases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information; Office of the Dir. of Nat'l Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act* (*FISA*) (Aug. 21, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-

(Continued on following page)

revealed other Government surveillance programs, including the Government's collection of internet data pursuant to a program called "PRISM." *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others,* GUARDIAN (London), June 6, 2013.[10]

Soon after the first public revelations in the news media, plaintiffs filed their complaints in these two cases on June 6, 2013 (*Klayman I*) and June 12, 2013 (*Klayman II*), alleging that the Government, with the participation of private companies, is conducting "a secret and illegal government scheme to intercept and analyze vast quantities of domestic telephonic communications," Second Am. Compl. ¶ 2 (*Klayman I*), and "of communications from the Internet and electronic service providers," Am. Compl. ¶ 2 (*Klayman II*). Plaintiffs in *Klayman I* – attorney Larry Klayman, founder of Freedom Watch, a public interest organization, and Charles Strange, the father of

---

intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa; Office of the Dir. of Nat'l Intelligence, *DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act* (*FISA*) (Sept. 10, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document; Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act (Aug. 9, 2013), *available at* http://apps.washingtonpost.com/g/page/politics/obama-administration-white-paper-on-nsa-surveillance-oversight/388/.

[10] *Available at* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Michael Strange, a cryptologist technician for the NSA and support personnel for Navy SEAL Team VI who was killed in Afghanistan when his helicopter was shot down in 2011 – assert that they are subscribers of Verizon Wireless and bring suit against the NSA, the Department of Justice ("DOJ"), and several executive officials (President Barack H. Obama, Attorney General Eric H. Holder, Jr., General Keith B. Alexander, Director of the NSA, and U.S. District Judge Roger Vinson), as well as Verizon Communications and its chief executive officer. Second Am. Compl. ¶¶ 9-19; Klayman Aff. ¶ 3; Strange Aff. ¶ 2. And plaintiffs in *Klayman II* – Mr. Klayman and Mr. Strange again, along with two private investigators, Michael Ferrari and Matthew Garrison – bring suit against the same Government defendants, as well as Facebook, Yahoo!, Google, Microsoft, YouTube, AOL, PalTalk, Skype, Sprint, AT & T, and Apple, asserting that plaintiffs are "subscribers, users, customers, and otherwise avail themselves to" these named internet and/or telephone service provider companies. Am. Compl. ¶¶ 1, 11-14; Klayman Aff. ¶ 3; Klayman Suppl. Aff. ¶ 3; Strange Aff. ¶ 3.[11] Specifically, plaintiffs allege that the Government has violated their individual rights under the First, Fourth, and Fifth Amendments of the Constitution and has violated the Administrative Procedure Act ("APA") by exceeding

[11] *See supra,* notes 5, 6.

its statutory authority under FISA.[12] Second Am. Compl. ¶¶ 1-8, 49-99.

I. Statutory Background

A. FISA and Section 215 of the USA PATRIOT Act (50 U.S.C. § 1861)

In 1978, Congress enacted the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 *et seq*. ("FISA"), "to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes." *Clapper v. Amnesty Int'l USA,* 133 S. Ct. 1138, 1143 (2013). Against the backdrop of findings by the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the "Church Committee") that the executive branch had, for decades, engaged in warrantless domestic intelligence-gathering activities that had illegally infringed the Fourth Amendment rights of American citizens, Congress passed FISA "in large measure [as] a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused." S. Rep. No. 95-604, at 7. In the view of the Senate Judiciary Committee, the act went "a long way in striking a fair

[12] Plaintiffs also allege certain statutory violations by the private company defendants, Second Am. Compl. ¶¶ 81-95, which are not at issue for purposes of the Preliminary Injunction Motions, as well as common law privacy tort claims, Second Am. Compl. ¶¶ 70-80.

and just balance between protection of national security and protection of personal liberties." *Id.* at 7.

FISA created a procedure for the Government to obtain ex parte judicial orders authorizing domestic electronic surveillance upon a showing that, *inter alia,* the target of the surveillance was a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1804(a)(3), 1805(a)(2). In enacting FISA, Congress also created two new Article III courts – the Foreign Intelligence Surveillance Court ("FISC"), composed of eleven U.S. district judges, "which shall have jurisdiction to hear applications for and grant orders approving" such surveillance, § 1803(a)(1), and the FISC Court of Review, composed of three U.S. district or court of appeals judges, "which shall have jurisdiction to review the denial of any application made under [FISA]," § 1803(b).[13]

[13] The eleven U.S. district judges are appointed by the Chief Justice of the United States to serve on the FISC for a term of seven years each. 50 U.S.C. § 1803(a)(1), (d). They are drawn from at least seven of the twelve judicial circuits in the United States, and at least three of the judges must reside within twenty miles of the District of Columbia. § 1803(a)(1). For these eleven district judges who comprise the FISC at any one time, their service on the FISC is *in addition to,* not in lieu of, their normal judicial duties in the districts in which they have been appointed. *See* Theodore W. Ruger, *Chief Justice Rehquist's Appointments to the FISA Court: An Empirical Perspective,* 101 NW. U.L. REV. 239, 244 (2007) ("Service on the FISA Court is a part-time position. The judges rotate through the court periodically and maintain regular district court caseloads in their home courts."). Accordingly, service on the FISC is, at best, a part-time

(Continued on following page)

In addition to authorizing wiretaps, §§ 1801-1812, FISA was subsequently amended to add provisions enabling the Government to obtain ex parte orders authorizing physical searches, §§ 1821-1829, as well as pen registers and trap-and-trace devices, §§ 1841-1846. *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807(a)(3), 108 Stat. 3423; Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601(2), 112 Stat. 2396 ("1999 Act"). In 1998, Congress added a "business records" provision to FISA. *See* 1999 Act § 602. Under that provision, the FBI was permitted to apply for an ex parte order authorizing specified entities, such as common carriers, to release to the FBI copies of business records upon a showing in the FBI's application that "there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." 50 U.S.C. § 1862(b)(2)(B) (2000).

Following the September 11, 2001 terrorist attacks, Congress passed the USA PATRIOT Act, which made changes to FISA and several other laws. Pub. L. No. 107-56, 115 Stat. 272 (2001). Section 215 of the

---

assignment that occupies a relatively small part of each judge's annual judicial duties. Further, as a result of the requirement that at least three judges reside within twenty miles of the nation's capital, a disproportionate number of the FISC judges are drawn from the district courts of the District of Columbia and the Eastern District of Virginia, *see id.* at 258 (Appendix) (listing Chief Justice Rehnquist's twenty-five appointments to the FISC, six of which came from the D.D.C. and E.D. Va.).

PATRIOT Act replaced FISA's business-records provision with a more expansive "tangible things" provision. Codified at 50 U.S.C. § 1861, it authorizes the FBI to apply "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." § 1861(a)(1). While this provision originally required that the FBI's application "shall specify that the records concerned are sought for" such an investigation, § 1861(b)(2) (Supp. I 2001), Congress amended the statute in 2006 to provide that the FBI's application must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." § 1861(b)(2)(A); *see* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192 ("USA PATRIOT Improvement and Reauthorization Act").

Section 1861 also imposes other requirements on the FBI when seeking to use this authority. For example, the investigation pursuant to which the request is made must be authorized and conducted under guidelines approved by the Attorney General under Executive Order No. 12,333 (or a successor

thereto). 50 U.S.C. § 1861(a)(2)(A), (b)(2)(A). And the FBI's application must "enumerat[e] . . . minimization procedures adopted by the Attorney General . . . that are applicable to the retention and dissemination by the [FBI] of any tangible things to be made available to the [FBI] based on the order requested." § 1861(b)(2)(B). The statute defines "minimization procedures" as, in relevant part, "specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting [U.S.] persons consistent with the need of the [U.S.] to obtain, produce, and disseminate foreign intelligence information." § 1861(g)(2). If the FISC judge finds that the FBI's application meets these requirements, he "shall enter an ex parte order as requested, or as modified, approving the release of tangible things" (hereinafter, "production order"). § 1861(c)(1); *see also* § 1861(f)(1)(A) ("the term 'production order' means an order to produce any tangible thing under this section").

Under Section 1861's "use" provision, information that the FBI acquires through such a production order "concerning any [U.S.] person may be used and disclosed by Federal officers and employees without the consent of the [U.S.] person only in accordance with the minimization procedures adopted" by the Attorney General and approved by the FISC. § 1861(h). Meanwhile, recipients of Section 1861 production

orders are obligated not to disclose the existence of the orders, with limited exceptions. § 1861(d)(1).

B. Judicial Review by the FISC

While the recipient of a production order must keep it secret, Section 1861 does provide the recipient – but only the recipient – a right of judicial review of the order before the FISC pursuant to specific procedures. Prior to 2006, recipients of Section 1861 production orders had no express right to judicial review of those orders, but Congress added such a provision when it reauthorized the PATRIOT Act that year. *See* USA PATRIOT Improvement and Reauthorization Act § 106(f); 1 D. KRIS & J. WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 19:7 (2d ed. 2012) ("Kris & Wilson") ("Prior to the Reauthorization Act in 2006, FISA did not allow for two-party litigation before the FISC").

Under Section 1861, "[a] person receiving a production order may challenge the legality of that order by filing a petition with the [petition review pool of FISC judges]." 50 U.S.C. § 1861(f)(2)(A)(i); *see* § 1803(e)(1).[14] The FISC review pool judge considering

[14] The three judges who reside within twenty miles of the District of Columbia comprise the petition review pool (unless all three are unavailable, in which case other FISC judges may be designated). § 1803(e)(1). In addition to reviewing petitions to review Section 1861 production orders pursuant to § 1861(f), the review pool also has jurisdiction to review petitions filed pursuant to § 1881a(h)(4). *Id.*

the petition may grant the petition "only if the judge finds that [the] order does not meet the requirements of [Section 1861] or is otherwise unlawful." § 1861(f)(2)(B). Once the FISC review pool judge rules on the petition, either the Government or the recipient of the production order may seek an en banc hearing before the full FISC, § 1803(a)(2)(A), or may appeal the decision by filing a petition for review with the FISC Court of Review, § 1861(f)(3). Finally, after the FISC Court of Review renders a written decision, either the Government or the recipient of the production order may then appeal this decision to the Supreme Court on petition for writ of certiorari. §§ 1861(f)(3), 1803(b). A production order "not explicitly modified or set aside consistent with [Section 1861(f)] shall remain in full effect." § 1861(f)(2)(D).

Consistent with other confidentiality provisions of FISA, Section 1861 provides that "[a]ll petitions under this subsection shall be filed under seal," § 1861(f)(5), and the "record of proceedings . . . shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence," § 1861(f)(4). *See also* § 1803(c).

II. Collection of Bulk Telephony Metadata Pursuant to Section 1861

To say the least, plaintiffs and the Government have portrayed the scope of the Government's surveillance activities very differently.[15] For purposes of resolving these preliminary injunction motions, however, as will be made clear in the discussion below, it will suffice to accept the Government's description of the phone metadata collection and querying program. *Cf. Cobell v. Norton,* 391 F.3d 251, 261 (D.C. Cir. 2004) (evidentiary hearing on preliminary injunction is necessary only if the court must make credibility determinations to resolve key factual disputes in favor of the *moving party*).

In broad overview, the Government has developed a "counterterrorism program" under Section 1861 in which it collect, compiles, retains, and analyzes certain telephone records, which it characterizes as "business records" created by certain telecommunications companies (the "Bulk Telephony Metadata Program"). The records collected under this program consist of "metadata," such as information about what phone numbers were used to make and receive calls,

---

[15] In addition to alleging that the NSA has "direct access" to Verizon's databases, Second Am. Compl. ¶ 7, and is collecting location information as part of "call detail records," Pls. Mem. at 10, Mr. Klayman and Mr. Strange also suggest that they are "prime target[s]" of the Government due to their public advocacy and claim that the Government is behind alleged inexplicable text messages being sent from and received on their phones, Pls.' Mem. at 13-16; Klayman Aff. ¶ 11; Strange Aff. ¶¶ 12-17.

when the calls took place, and how long the calls lasted. Decl. of Acting Assistant Director Robert J. Holley, Federal Bureau of Investigation ("Holley Decl.") [Dkt. # 25-5], at ¶ 5; Decl. of Teresa H. Shea, Signals Intelligence Director, National Security Agency ("Shea Decl.") [Dkt. # 25-4], at ¶ 7; Primary Order, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things From [Redacted],* No. BR 13-158 at 3 n.1 (FISC Oct. 11, 2013) (attached as Ex. B to Gilligan Decl.) [Dkt. # 25-3] ("Oct. 11, 2013 Primary Order").[16] According to the representations made by the Government, the metadata records collected under the program do *not* include *any* information about the content of those calls, or the names, addresses, or financial information of any party to the calls. Holley Decl. ¶¶ 5, 7; Shea Decl. ¶ 15; Oct. 11, 2013 Primary Order at 3 n.1.[17] Through targeted computerized searches of

[16] Oct. 11, 2013 Primary Order at 3 n.1 ("For purposes of this Order 'telephony metadata' includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.").

[17] Plaintiffs have alleged that the Government has also collected location information for cell phones. Second Am. Comp. ¶ 28; Pls.' Mem. at 10-11. While more recent FISC opinions expressly state that cell-site location information is not covered by Section 1861 production orders, *see, e.g.,* Oct. 11, 2013 Primary Order at 3 n.1, the Government has *not* affirmatively represented to this Court that the NSA has *not,* at any point in the

(Continued on following page)

those metadata records, the NSA tries to discern connections between terrorist organizations and previously unknown terrorist operatives located in the United States. Holley Decl. ¶ 5; Shea Decl. ¶¶ 8-10, 44.

The Government has conducted the Bulk Telephony Metadata Program for more than seven years. Beginning in May 2006 and continuing through the present,[18] the FBI has obtained production orders from the FISC under Section 1861 directing certain telecommunications companies to produce, on an ongoing daily basis, these telephony metadata records, Holley Decl. ¶ 6; Shea Decl. ¶ 13, which the companies create and maintain as part of their business of providing telecommunications services to customers, Holley Decl. ¶ 10; Shea Decl. ¶ 18. The NSA then consolidates the metadata records

---

history of the Bulk Telephony Metadata Program, collected location information (in one technical format or another) about cell phones. *See, e.g.,* Govt's Opp'n at 9 (defining telephony metadata and noting what is not included); Order, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from [Redacted],* No. BR 06-05 at 2 (FISC May 24, 2006), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document (defining telephony metadata and noting what is not included, but *not* expressly stating that the order does *not* authorize the production of cell-site location information).

[18] The most recent FISC order authorizing the Bulk Telephony Metadata Program that the Government has disclosed (in redacted form, directed to an unknown recipient) expires on January 3, 2014. *See* Oct. 11, 2013 Primary Order at 17.

provided by different telecommunications companies into one database, Shea Decl. ¶ 23, and under the FISC's orders, the NSA may retain the records for up to five years, *id.* ¶ 30; *see* Oct. 11, 2013 Primary Order at 14. According to Government officials, this aggregation of records into a single database creates "an historical repository that permits retrospective analysis," Govt's Opp'n at 12, enabling NSA analysts to draw connections, across telecommunications service providers, between numbers reasonably suspected to be associated with terrorist activity and with other, unknown numbers. Holley Decl. ¶¶ 5, 8; Shea Decl. ¶¶ 46, 60.

The FISC orders governing the Bulk Telephony Metadata Program specifically provide that the metadata records may be accessed only for counterterrorism purposes (and technical database maintenance). Holley Decl. ¶ 8; Shea Decl. ¶ 30. Specifically, NSA intelligence analysts, *without seeking the approval of a judicial officer,* may access the records to obtain foreign intelligence information only through "queries" of the records performed using "identifiers," such as telephone numbers, associated with terrorist activity.[19] An "identifier" (i.e., selection term, or search

[19] In her declaration, Teresa H. Shea, Director of the Signals Intelligence Directorate at the NSA, states that "queries," or "term searches," of the metadata database are conducted "using metadata 'identifiers,' *e.g., telephone numbers,* that are associated with a foreign terrorist organization." Shea Decl. ¶ 19 (emphasis added). If a telephone number is only an *example* of an identifier that may be used as a search term, it is not clear

(Continued on following page)

term) used to start a query of the database is called a "seed," and "seeds" must be approved by one of twenty-two designated officials in the NSA's Homeland Security Analysis Center or other parts of the NSA's Signals Intelligence Directorate. Shea Decl. ¶¶ 19, 31. Such approval may be given only upon a determination by one of those designated officials that there exist facts giving rise to a "reasonable, articulable suspicion" ("RAS") that the selection term to be queried is associated with one or more of the specified foreign terrorist organizations approved for targeting by the FISC. Holley Decl. ¶¶ 15-16.[20] In 2012, for example, fewer than 300 unique identifiers met this RAS standard and were used as "seeds" to query the metadata, but "the number of unique identifiers has varied over the years." Shea Decl. ¶ 24.

When an NSA intelligence analyst runs a query using a "seed," the minimization procedures provide that query results are limited to records of communications within three "hops" from the seed. *Id.* ¶ 22. The query results thus will include only identifiers and their associated metadata having a direct contact

---

what other "identifiers" may be used to query the database, and the Government has not elaborated. *See, e.g.,* Oct. 11, 2013 Primary Order at 5 n.4, 7-10 (redacting text that appears to discuss "selection terms").

[20] A determination that a selection term meets the RAS standard remains effective for 180 days for any selection term reasonably believed to be used by a U.S. person, and for one year for all other selection terms. *See* Oct. 11, 2013 Primary Order at 10.

with the seed (the first "hop"), identifiers and associated metadata having a direct contact with first "hop" identifiers (the second "hop"), and identifiers and associated metadata having a direct contact with second "hop" identifiers (the third "hop"). *Id.* ¶ 22; Govt's Opp'n at 11. In plain English, this means that if a search starts with telephone number (123) 456-7890 as the "seed," the first hop will include all the phone numbers that (123) 456-7890 has called or received calls from in the last five years (say, 100 numbers), the second hop will include all the phone numbers that each of *those* 100 numbers has called or received calls from in the last five years (say, 100 numbers for each one of the 100 "first hop" numbers, or 10,000 total), and the third hop will include all the phone numbers that each *of those* 10,000 numbers has called or received calls from in the last five years (say, 100 numbers for each one of the 10,000 "second hop" numbers, or 1,000,000 total). *See* Shea Decl. ¶ 25 n.1. The actual number of telephone numbers and their associated metadata captured in any given query varies, of course, but in the absence of any specific representations from the Government about typical query results, it is likely that the quantity of phone numbers captured in any given query would be very large.[21]

---

[21] After stating that fewer than 300 unique identifiers met the RAS standard and were used as "seeds" to query the metadata in 2012, Ms. Shea notes that "[b]ecause the same seed identifier can be queried more than once over time, can generate

(Continued on following page)

multiple responsive records, and can be used to obtain contact numbers up to three 'hops' from the seed identifier, the number of metadata records responsive to such queries is *substantially larger than 300, but is still a very small percentage of the total volume of metadata records*." Shea Decl. ¶ 24 (emphasis added). The first part of this assertion is a glaring understatement, while the second part is virtually meaningless when placed in context. First, as the sample numbers I have used in the text above demonstrate, it is possible to arrive at a query result in the millions within three hops while using even conservative numbers – needless to say, this is "substantially larger than 300." After all, even if the average person in the United States does not call or receive calls from 100 unique phone numbers in one year, what about over a five-year period? And second, it belabors the obvious to note that even a few million phone numbers is "a very small percentage of the total volume of metadata records" if the Government has collected metadata records on hundreds of millions of phone numbers.

But it's also easy to imagine the spiderweb-like reach of the three-hop search growing exponentially and capturing even higher numbers of phone numbers. Suppose, for instance, that there is a person living in New York City who has a phone number that meets the RAS standard and is approved as a "seed." And suppose this person, who may or may not actually be associated with any terrorist organization, calls or receives calls from 100 unique numbers, as in my example. But now suppose that one of the numbers he calls is his neighborhood Domino's Pizza shop. The Court won't hazard a guess as to how many different phone numbers might dial a given Domino's Pizza outlet in New York City in a five-year period, but to take a page from the Government's book of understatement, it's "substantially larger" than the 100 in the second hop of my example, and would therefore most likely result in exponential growth in the scope of the query and lead to millions of records being captured by the third hop. (I recognize that some minimization procedures described in recent FISC orders permitting technical personnel to access the metadata database to "defeat [ ] high volume and other unwanted [ ] metadata," Oct. 11, 2013 Primary Order at 6,

(Continued on following page)

Once a query is conducted and it returns a universe of responsive records (i.e., a universe limited to records of communications within three hops from the seed), trained NSA analysts may then perform new searches and otherwise perform intelligence analysis *within* that universe of data without using RAS-approved search terms. *See* Shea Decl. ¶ 26 (NSA analysts may "chain contacts within the query results themselves"); Oct. 11, 2013 Primary Order.[22] According to the Government, following the "chains of communication" – which, for chains that cross different communications networks, is only possible

---

may, in practice, reduce the likelihood of my Domino's hypothetical example occurring. But, of course, that does not change the baseline fact that, by the terms of the FISC's orders, the NSA is permitted to run queries capturing up to three hops that can conceivably capture millions of Americans' phone records. Further, these queries using non-RAS-approved selection terms, which are permitted to make the database "usable for intelligence analysis," *id.* at 5, may very well themselves involve searching across millions of records.)

[22] Under the terms of the most recent FISC production order available, "[q]ueries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below. This automated query process queries the collected BR metadata (in a 'collection store') with RAS-approved selection terms and returns the hop-limited results from those queries to a 'corporate store.' The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms." Oct. 11, 2013 Primary Order at 11 (footnote omitted). This "automated query process" was first approved by the FISC in a November 8, 2012 order. *Id.* at 11 n.11.

if the metadata is aggregated – allows the analyst to discover information that may not be readily ascertainable through other, targeted intelligence-gathering techniques. Shea Decl. ¶ 46. For example, the query might reveal that a seed telephone number has been in contact with a previously unknown U.S. telephone number – i.e., on the first hop. *See id.* ¶ 58. And from there, "contact-chaining" out to the second and third hops to examine the contacts made by that telephone number may reveal a contact with other telephone numbers already known to the Government to be associated with a foreign terrorist organization. *Id.* ¶¶ 47, 62. In short, the Bulk Telephony Metadata Program is meant to detect: (1) domestic U.S. phone numbers calling *outside* of the U.S. to foreign phone numbers associated with terrorist groups; (2) foreign phone numbers associated with terrorist groups calling *into* the U.S. to U.S. phone numbers; and (3) "possible terrorist-related communications" between U.S. phone numbers *inside* the U.S. *See id.* ¶ 44.

Since the program began in May 2006, the FISC has repeatedly approved applications under Section 1861 and issued orders directing telecommunications service providers to produce records in connection with the Bulk Telephony Metadata Program. Shea Decl. ¶¶ 13-14. Through October 2013, fifteen different FISC judges have issued thirty-five orders authorizing the program. Govt's Opp'n at 9; *see also* Shea Decl. ¶ 13-14; Holley Decl. ¶ 6. Under those orders, the Government must periodically seek renewal of the authority to collect telephony records (typically

every ninety days). Shea Decl. ¶ 14. The Government has nonetheless acknowledged, as it must, that failures to comply with the minimization procedures set forth in the orders have occurred. For instance, in January 2009, the Government reported to the FISC that the NSA had improperly used an "alert list" of identifiers to search the bulk telephony metadata, which was composed of identifiers that had *not* been approved under the RAS standard. *Id.* ¶ 37; Order, *In re Production of Tangible Things from [Redacted],* No. BR 08-13, 2009 WL 9150913, at *2 (FISC Mar. 2, 2009) ("Mar. 2, 2009 Order"). After reviewing the Government's reports on its noncompliance, Judge Reggie Walton of the FISC concluded that the NSA had engaged in "systematic noncompliance" with FISC-ordered minimization procedures over the preceding three years, since the inception of the Bulk Telephony Metadata Program, and had also repeatedly made misrepresentations and inaccurate statements about the program to the FISC judges. Mar. 2, 2009 Order, 2009 WL 9150913, at *2-5.[23] As a consequence, Judge

[23] Judge Walton noted that, "since the earliest days of the FISC-authorized collection of call-detail records by the NSA, the NSA has on a daily basis, accessed the BR metadata for purposes of comparing thousands of non-RAS-approved telephone identifiers on its alert list against the BR metadata in order to identify any matches. Such access was prohibited by the governing minimization procedures under each of the relevant Court orders." Mar. 2, 2009 Order, 2009 WL 9150913, at *2. He went on to conclude: "In summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of

(Continued on following page)

Walton concluded that he had no confidence that the Government was doing its utmost to comply with the court's orders, and ordered the NSA to seek FISC approval on a *case-by-case basis* before conducting any further queries of the bulk telephony metadata collected pursuant to Section 1861 orders. *Id.* at *9; Shea Decl. ¶¶ 38-39. This approval procedure remained in place from March 2009 to September 2009. Shea Decl. ¶¶ 38-39.

Notwithstanding this six-month "sanction" imposed by Judge Walton, the Government apparently has had further compliance problems relating to its collection programs in subsequent years. In October 2011, the Presiding Judge of the FISC, Judge John Bates, found that the Government had misrepresented the scope of its targeting of certain internet communications pursuant to 50 U.S.C. § 1881a (i.e., a different collection program than the Bulk Telephony Metadata Program at issue here). Referencing the 2009 compliance issue regarding the NSA's use of unauthorized identifiers to query the metadata in the

---

how the NSA uses BR metadata. This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively." *Id.* at *5.

Bulk Telephony Metadata Program, Judge Bates wrote: "the Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program." Mem. Op., *[Redacted],* No. [redacted], at 16 n.14 (FISC Oct. 3, 2011).[24] Both Judge Walton's and Judge Bates's opinions were only recently declassified by the Government in response to the Congressional and public reaction to the Snowden leaks.[25]

---

[24] *Available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa. Whatever the second "substantial misrepresentation" was, the Government appears to have redacted it from the footnote in that opinion.

[25] *See* Office of the Dir. of Nat'l Intelligence, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act* (FISA) (Aug. 21, 2013), available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa; Office of the Dir. of Nat'l Intelligence, *DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act* (*FISA*) (Sept. 10, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/927-draft-document.

ANALYSIS

I will address plaintiffs' statutory claim under the APA before I turn to their constitutional claim under the Fourth Amendment.

I. Statutory Claim Under the APA

Invoking this Court's federal question jurisdiction under 28 U.S.C. § 1331, plaintiffs allege that the Government's phone metadata collection and querying program exceeds the statutory authority granted by FISA's "tangible things" provision, 50 U.S.C. § 1861, and thereby violates the Administrative Procedure Act ("APA"), 5 U.S.C. § 706. *See* Second Am. Compl. ¶¶ 96-99; Pls.' Mem. at 2, 17-19; Pls.' Reply in Supp. of Mots. for Prelim. Inj. ("Pls.' Reply") [Dkt. # 31], at 5-11. In particular, plaintiffs argue that the bulk records obtained under the Bulk Telephony Metadata Program are not "relevant" to authorized national security investigations, *see* 50 U.S.C. § 1861(b)(2)(A), and that the FISC may not prospectively order telecommunications service providers to produce records that do not yet exist. *See* Pls.' Mem. at 17-19; Pls.' Reply at 5-11. In response, the Government argues that this Court lacks subject matter jurisdiction over this statutory claim because Congress impliedly precluded APA review of such claims. Government Defs.' Supplemental Br. in Opposition to Pls.' Mots. Prelim. Inj. ("Govt's Suppl. Br.") [Dkt. # 43], at 2. For the following reasons, I agree

with the Government that I am precluded from reviewing plaintiffs' APA claim.

The APA "establishes a cause of action for those 'suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action.'" *Koretoff v. Vilsack,* 614 F.3d 532, 536 (D.C. Cir. 2010) (quoting 5 U.S.C. § 702). In particular, the APA permits such aggrieved persons to bring suit against the United States and its officers for "relief other than money damages," 5 U.S.C. § 702, such as the injunctive relief plaintiffs seek here. This general waiver of sovereign immunity does not apply, however, "if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought." *Id.* Similarly the APA's "basic presumption of judicial review [of agency action]," *Abbott Labs v. Gardner,* 387 U.S. 136, 140 (1967), does not apply "to the extent that . . . statutes preclude judicial review," 5 U.S.C. § 701(a)(1). Accordingly, "[t]he presumption favoring judicial review of administrative action is just that – a presumption," *Block v. Community Nutrition Inst.,* 467 U.S. 340, 349 (1984), and it may be overcome "whenever the congressional intent to preclude judicial review is 'fairly discernible in the statutory scheme.'" *Id.* at 351. Assessing "[w]hether a statute precludes judicial review of agency action . . . is a question of congressional intent, which is determined from the statute's 'express language,' as well as 'from the structure of the statutory scheme, its objectives, its legislative history, and the nature of the administrative action involved.'" *Koretoff,* 614 F.3d at

536 (quoting *Block,* 467 U.S. at 345); *see also Thunder Basin Coal Co. v. Reich,* 510 U.S. 200, 207 (1994).

The Government insists that two statutes – 50 U.S.C. § 1861, the "tangible things" provision of FISA itself, and 18 U.S.C. § 2712, a provision of the USA PATRIOT Act, codified in the Stored Communications Act – *impliedly* preclude this Court's review of plaintiffs' statutory APA claim. Govt's Opp'n at 26-31; Govt's Suppl. Br. at 1-4. The text of Section 1861, and the structure and purpose of the FISA statutory scheme, as a whole, do indeed reflect Congress's preclusive intent. Stated simply, Congress created a closed system of judicial review of the government's domestic foreign intelligence-gathering, generally, 50 U.S.C. § 1803, and of Section 1861 production orders, specifically, § 1861(f). This closed system includes no role for third parties, such as plaintiffs here, nor courts besides the FISC, such as this District Court. Congress's preclusive intent is therefore sufficiently clear. How so?

First, and most directly, the text of the applicable provision of FISA itself, Section 1861, evinces Congress's intent to preclude APA claims like those brought by plaintiffs before this Court. Section 1861 expressly provides a right of judicial review of orders to produce records, but it only extends that right to the *recipients* of such orders, such as telecommunications service providers. *See* 50 U.S.C. § 1861(f). Congress thus did *not* preclude *all* judicial review of Section 1861 production orders, but I, of course, must determine "whether Congress nevertheless foreclosed

review to the class to which the [plaintiffs] belon[g]." *Block,* 467 U.S. at 345-46. And "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." *Id.* at 349 (emphases added); *see also id.* at 345-48 (holding that the statutory scheme of the Agricultural Marketing Agreement Act ("AMAA"), which expressly provided a mechanism for milk *handlers* to obtain judicial review of milk market orders issued by the Secretary of Agriculture, impliedly precluded review of those orders in suits brought by milk *consumers*). That is exactly the case here. Congress has established a detailed scheme of judicial review of the particular issue of the "legality" of Section 1861 production orders at the behest of only recipients of those orders. 50 U.S.C. §§ 1861(f)(2)(A)(i) ("A person receiving a production order may challenge the *legality* of that order by filing a petition with the [petition review pool of FISC judges]." (emphasis added)), 1861(f)(2)(B) ("A judge considering a petition to modify or set aside a production order may grant such petition only if the judge finds that such order *does not meet the requirements of this section or is otherwise unlawful*." (emphasis added)). And that scheme of judicial review places such challenges before the FISC: Section 1861 permits such challenges to be heard only by the petition review pool of the FISC. *See* § 1861(f)(2)(A)(i); § 1803(e)(1) (the FISC petition review pool "shall have jurisdiction to review petitions filed pursuant to section 1861(f)(1) . . . of this title").

Second, the purpose and legislative history of Section 1861 also support the conclusion that Congress intended to preclude APA claims by third parties. Simply put, Congress did not envision that third parties, such as plaintiffs, would even *know* about the existence of Section 1861 orders, much less challenge their legality under the statute. *See, e.g.,* H.R. Rep. No. 109-174 at 128, 268 (2005). As the Government points out, "Section [1861], like other provisions of FISA, establishes a secret and expeditious process that involves only the Government and the recipient of the order" in order to "promote its effective functioning as a tool for counter-terrorism." Govt.'s Opp'n at 29; *see also* 50 U.S.C. § 1861(d)(1) (recipient of production order may not "disclose to any other person that the [FBI] has sought or obtained" an order under Section 1861); § 1861(f)(5) ("All petitions under this subsection shall be filed under seal."); § 1861(f)(4) ("The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence."). Congress did think about third parties, such as persons whose records would be targeted, when it created a right to judicial review of Section 1861 production orders for recipients, but it recognized that extending a similar right to third parties

would make little sense in light of the secrecy of such orders. *See* H.R. Rep. No. 109-174 at 128, 268; Govt's Opp'n at 29 n.14; Govt's Suppl. Br. at 3.[26] Congress therefore considered the precise issue of challenges to the legality of Section 1861 orders, and the statute reflects its ultimate conclusions as to who may seek review and in what court. § 1861(f); *see also* H.R. Rep. No. 109-174 at 128-29, 134, 137 (rejecting amendment that would have allowed recipients of Section 1861 orders to bring challenges to such orders in federal district court).

But even setting aside the specific fact that FISA does not contain a judicial review provision for third parties regarding Section 1861 orders, Congress's preclusive intent is all the more evident when one considers, viewing FISA as a whole, that Congress did not contemplate the participation of third parties in the statutory scheme *at all*. *See Ark. Dairy Coop. Ass'n v. Dep't of Agric.,* 573 F.3d 815, 822 (D.C. Cir. 2009) (noting that in reaching its decision in *Block,* "the Supreme Court did not concentrate simply on the

[26] Congress has also not provided a suppression remedy for tangible things obtained under Section 1861, in contrast to the "use of information" provisions under nearly every other subchapter of FISA, which contain such a remedy. *Compare* 50 U.S.C. § 1861 *with* §§ 1806(e) (evidence obtained or derived from an electronic surveillance), 1825(f) (evidence obtained or derived from a physical search), 1845(e) (evidence obtained or derived from the use of a pen register or trap and trace device), 1881e (deeming information acquired under the section to be acquired "from an electronic surveillance" for purposes of Section 1806).

presence or absence of an explicit right of appeal [for consumers] in the AMAA, but instead noted that in the 'complex scheme' of the AMAA, there was no provision for consumer participation of any kind.").[27] Indeed, until 2006, FISA did not expressly contemplate participation by even the *recipients* of Section 1861 production orders, let alone third parties. Rather, as originally enacted, FISA was characterized by a secret, ex parte process in which only the government participated. Period. *See* 50 U.S.C. § 1805(a),

[27] In *Arkansas Dairy,* our Circuit Court addressed a suit concerning the AMAA, the same statute at issue in *Block*. The government, relying on *Block* 's holding that milk *consumers* were barred from bringing a claim because the statute did not grant them an express right to judicial review, argued that *milk producers* likewise could not bring an action because the AMAA did not provide them an express right to judicial review either. *See Ark. Dairy,* 573 F.3d at 822. While our Circuit Court rejected this argument, stating that "this approach reads *Block* too broadly," it reasoned that "the Supreme Court [in *Block*] did not concentrate simply on the presence or absence of an explicit right of appeal in the AMAA, but instead noted that in the 'complex scheme' of the AMAA, there was no provision for consumer participation of any kind." *Id.* In that particular case, our Circuit Court found that the AMAA did, in fact, contemplate the participation of milk producers in the regulatory process, and the court relied on this factor, in part, in holding that producers could bring suit under the APA. *Id.* at 822-27. Here, by contrast, the FISA statutory scheme does not contemplate any participation by third parties in the process of regulating governmental surveillance for foreign intelligence purposes, nor does Section 1861 contemplate the participation of third parties in adjudicating the legality of production orders. Indeed, only in the last decade has the FISA statutory scheme permitted participation by even recipients of production orders.

(e)(4); *In re Sealed Case,* 310 F.3d 717, 719 (FISA Ct. Rev. 2002) ("[T]he government is the only party to FISA proceedings. . . ."). In passing the USA PATRIOT Improvement and Reauthorization Act, however, Congress provided an avenue for recipients of Section 1861 production orders to participate in litigation before the FISC and thus play a role in the statutory scheme. *See* USA PATRIOT Improvement and Reauthorization Act § 106(f); Kris & Wilson, § 19:7.[28] As such, it would not be prudent to treat Congressional silence regarding third parties as an intent to provide broader judicial review than that specifically set forth in the statute.[29] Judicial alchemy of that sort is

[28] The USA PATRIOT Improvement and Reauthorization Act also added a provision allowing recipients of National Security Letters ("NSLs") to seek judicial review of those letters. *See* USA PATRIOT Improvement and Reauthorization Act § 115. In contrast to the provision of a right of judicial review to recipients of Section 1861 production orders *before the FISC,* the act provided that the recipient of an NSL (under any of the five NSL statutes) "may, in the United States district court for the district in which that person or entity does business or resides, petition for an order modifying or setting aside the request." 18 U.S.C. § 3511.

[29] Indeed, it would be curious to reach the opposite conclusion – that even though the statute expressly permits only recipients to challenge Section 1861 production orders in a specific forum (after Congress rejected an amendment that proposed to allow them to bring their challenges in federal district court at the same time it decided to allow recipients of NSLs to do exactly that), and even though Congress considered but declined to extend that right of judicial review to third parties, *see* Govt's Suppl. Br. at 3, these plaintiffs can nonetheless, in effect, challenge those orders in district court by bringing a claim under the APA challenging government agency conduct. In *Block,* when

(Continued on following page)

particularly inappropriate on matters affecting national security.

To be sure, FISA and Section 1861 *do* implicate the interests of cell phone subscribers when their service providers are producing metadata about their phone communications to the Government, as I will discuss below in the context of plaintiffs' constitutional claims. But the statutory preclusion inquiry "does not only turn on whether the interests of a particular class . . . are implicated." *Block,* 467 U.S. at 347. "Rather, the preclusion issue turns ultimately on whether Congress intended for that class to be relied upon to challenge agency disregard of the law." *Id.* Here, the detailed procedures set out in the statute for judicial review of Section 1861 production orders, at the behest of recipients of those orders, indicate

---

finding that the AMAA statute precluded claims by milk consumers, the Supreme Court noted that permitting consumers to seek judicial review of milk orders directly when the statute required milk handlers to first exhaust administrative remedies, "would severely disrupt this complex and delicate administrative scheme." *Block,* 467 U.S. at 348; *cf. Sackett v. EPA,* 132 S. Ct. 1367, 1374 (2012) ("Where a statute provides that particular agency action is reviewable at the instance of one party, who must first exhaust administrative remedies, the inference that it is not reviewable at the instance of other parties, who are not *subject* to the administrative process, is strong."). Permitting third parties to come into federal district court to challenge the legality of Section 1861 production orders, or government agency action conducted pursuant thereto, under the banner of an APA claim would likewise frustrate the statutory scheme here, where Congress in FISA has set out a specific process for judicial review of those orders by the FISC.

that, for better or worse, Congress did not intend for third parties, such as plaintiff phone subscribers here, to challenge the Government's compliance with the statute.[30]

---

[30] Finally, against this backdrop of FISA's structure, purpose, and history, I find the Government's second preclusion argument – that 18 U.S.C. § 2712 also shows Congress's intent to preclude an APA statutory claim under Section 1861, Govt's Opp'n at 30 – more persuasive than it otherwise appears when reading that statute alone. Section 2712, which Congress added to the Stored Communications Act in 2001, provides that "[a]ny person who is aggrieved by any willful violation of [the Stored Communications Act] or of [the Wiretap Act] or of sections 106(a) [50 U.S.C. § 1806(a)], 305(a) [50 U.S.C. § 1825(a)], or 405(a) [50 U.S.C. § 1845(a)] of the Foreign Intelligence Surveillance Act . . . may commence an action in United States District Court against the United States to recover money damages." The Government argues that because this statute creates a *money damages* action against the United States for violations of three specific provisions of FISA, it impliedly precludes an action for *injunctive relief* regarding *any* provision of FISA, such as Section 1861. *See* Govt's Opp'n at 30-31; Govt's Suppl. Br. at 3-4. According to the Government, "Section 2712 thus deals with claims for misuses of information obtained under FISA in great detail, including the intended remedy," and therefore plaintiffs here cannot rely on Section 1861 "to bring a claim for violation of FISA's terms that Congress did not provide for under 18 U.S.C. § 2712." Govt's Opp'n at 31. Indeed, Judge White in the Northern District of California came to this same conclusion, holding that Section 2712, "by allowing suits against the United States only for damages based on three provisions of [FISA], impliedly bans suits against the United States that seek injunctive relief under any provision of FISA." *Jewel v. Nat'l Sec. Agency,* ___ F. Supp. 2d ___, 2013 WL 3829405, at *12 (N.D. Cal. July 23, 2013). Of course, Section 2712 also expressly provides that "[a]ny action against the United States under this subsection shall be the exclusive remedy against the United States for any claims *within*

(Continued on following page)

II. Constitutional Claims

A. Jurisdiction

Finding that I lack jurisdiction to review plaintiffs' APA claim does not, however, end the Court's jurisdictional inquiry. Plaintiffs have raised several constitutional challenges to the Government's conduct at issue here. And while the Government has conceded this Court's authority to review these constitutional claims, Govt's Suppl. Br. at 4, I must nonetheless independently evaluate my jurisdictional authority, *see Henderson ex rel. Henderson v. Shinseki,* 131 S. Ct. 1197, 1202 (2011) ("[F]ederal courts have an independent obligation to ensure that they do not exceed the scope of their jurisdiction, and therefore they must raise and decide jurisdictional questions that the parties either overlook or elect not to press.").

---

the purview of this section," 18 U.S.C. § 2712(d) (emphasis added), and therefore it might be argued that Section 2712's provision of a remedy should not be read more broadly to have any preclusive impact on violations of other provisions of FISA, such as Section 1861, not "within the purview" of that section. But when read in conjunction with FISA overall, and in light of the secret nature of FISA proceedings designed to advance intelligence-gathering for national security purposes, I agree with the Government that Section 2712's provision of a certain remedy, money damages, for violations of only certain provisions of FISA should be read to further show Congress's intent to preclude judicial review of APA claims for injunctive relief by third parties regarding any provision of FISA, including Section 1861.

Because Article III courts were created, in part, to deal with allegations of constitutional violations, U.S. CONST. art. III, § 2, the jurisdictional inquiry here turns, in the final analysis, on whether Congress intended to preclude judicial review of constitutional claims related to FISC orders by any non-FISC courts. Not surprisingly, the Supreme Court has addressed Congressional efforts to limit constitutional review by Article III courts. In *Webster v. Doe,* 486 U.S. 592 (1988), the Court stated emphatically that "where Congress intends to preclude judicial review of constitutional claims its intent to do so must be clear." *Id.* at 603. Such a "heightened showing" is required "in part to avoid the 'serious constitutional question' that would arise if a federal statute were construed to deny any judicial forum for a colorable constitutional claim." *Id.* (holding that although a former CIA employee who alleged that he was fired because he was a homosexual, in violation of the APA and the Constitution, could not obtain judicial review under the APA because such decisions were committed to the agency's discretion by law, 5 U.S.C. § 701(a)(2), under a provision of the National Security Act of 1947, a court could nonetheless review the plaintiff's constitutional claims based on the same allegation).

As discussed in Part I above, FISA does not include an express right of judicial review for third party legal challenges to Section 1861 orders – whether constitutional or otherwise, whether in the FISC or elsewhere. But neither does FISA contain any language *expressly barring* all judicial review of third

party claims regarding Section 1861 orders – a necessary condition to even raise the question of whether FISA's statutory scheme of judicial review provides the exclusive means of review for constitutional claims relating to Section 1861 production orders. *See Elgin v. Dep't of the Treasury,* 132 S. Ct. 2126, 2132 (2012) ("[A] necessary predicate to the application of *Webster*'s heightened standard [is] a statute that purports to 'deny any judicial forum for a colorable constitutional claim.'"); *see also McBryde v. Comm. to Review Circuit Council Conduct & Disability Orders of the Judicial Conference of U.S.,* 264 F.3d 52, 59 (D.C. Cir. 2001) (the D.C. Circuit "find[s] preclusion of review for both as applied and facial constitutional challenges only if the evidence of congressional intent to preclude is 'clear and convincing'. . . . [and] we have not regarded broad and seemingly comprehensive statutory language as supplying the necessary clarity to bar as applied constitutional claims"); *Ungar v. Smith,* 667 F.2d 188, 193-96 (D.C. Cir. 1981) (holding that statutory language in 22 U.S.C. § 1631o(c) stating administrative determinations "shall be final and shall not be subject to review by any court" did *not* bar courts from hearing constitutional claims relating to the statute, absent a clear expression of Congress's intent to bar such claims in the statute's legislative history). Because FISA contains no "broad and seemingly comprehensive statutory language" expressly barring judicial review of *any* claims under Section 1861, let alone any language directed at *constitutional* claims in particular, Congress has *not* demonstrated an intent to preclude constitutional claims

sufficient to even trigger the *Webster* heightened standard in the first place, let alone "clear" enough to meet it.

This, of course, makes good sense. The presumption that judicial review of constitutional claims is available in federal district courts is a strong one, *Webster,* 486 U.S. at 603, and if the *Webster* heightened standard is to mean anything, it is that Congress's intent to preclude review of constitutional claims must be much clearer than that sufficient to show *implied* preclusion of *statutory* claims. Where, as here, core individual constitutional rights are implicated by Government action, Congress should not be able to cut off a citizen's right to judicial review of that Government action simply because it intended for the conduct to remain secret by operation of the design of its statutory scheme. While Congress has great latitude to create statutory schemes like FISA, it may not hang a cloak of secrecy over the Constitution.

B. Preliminary Injunction

When ruling on a motion for preliminary injunction, a court must consider "whether (1) the plaintiff has a substantial likelihood of success on the merits; (2) the plaintiff would suffer irreparable injury were an injunction not granted; (3) an injunction would substantially injure other interested parties; and (4) the grant of an injunction would further the public interest." *Sottera, Inc. v. Food & Drug Admin.,* 627

F.3d 891, 893 (D.C. Cir. 2010) (internal quotation marks omitted).[31] I will address each of these factors in turn.

1. Plaintiffs Have Shown a Substantial Likelihood of Success on the Merits.

In addressing plaintiffs' likelihood of success on the merits of their constitutional claims, I will focus on their Fourth Amendment arguments, which I find to be the most likely to succeed.[32] First, however, I must address plaintiffs' standing to challenge the various aspects of the Bulk Telephony Metadata Program. *See Jack's Canoes & Kayaks, LLC v. Nat'l Park Serv.,* 933 F. Supp. 2d 58, 76 (D.D.C. 2013) ("The first component of the likelihood of success on the merits

---

[31] Our Circuit has traditionally applied a "sliding scale" approach to these four factors. *Davis v. Pension Benefit Guar. Corp.,* 571 F.3d 1288, 1291 (D.C. Cir. 2009). In other words, "a strong showing on one factor could make up for a weaker showing on another." *Sherley v. Sebelius,* 644 F.3d 388, 392 (D.C. Cir. 2011). Following the Supreme Court's decision in *Winter v. NRDC, Inc.,* 555 U.S. 7 (2008), however, our Circuit "has suggested, without deciding, that *Winter* should be read to abandon the sliding-scale analysis in favor of a 'more demanding burden' requiring Plaintiffs to independently demonstrate both a likelihood of success on the merits and irreparable harm." *Smith v. Henderson,* ___ F. Supp. 2d ___, 2013 WL 2099804, at *4 (D.D.C. May 15, 2013) (citing *Sherley,* 644 F.3d at 392). Regardless of how *Winter* is read, the Court's analysis here is unaffected because I conclude that plaintiffs have made a sufficient showing of both a likelihood of success on the merits and irreparable harm.

[32] *See supra* note 7.

prong usually examines whether the plaintiffs have standing in a given case." (internal quotation marks omitted)).

a. Plaintiffs Have Standing to Challenge Bulk Telephony Metadata Collection and Analysis.

"To establish Article III standing, an injury must be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Clapper v. Amnesty Int'l USA,* 133 S. Ct. 1138, 1147 (2013) (internal quotation marks omitted). In *Clapper,* the Supreme Court held that plaintiffs lacked standing to challenge NSA surveillance under FISA because their "highly speculative fear" that they would be targeted by surveillance relied on a "speculative chain of possibilities" insufficient to demonstrate a "certainly impending" injury. *Id.* at 1147-50. Moreover, the *Clapper* plaintiffs' "self-inflicted injuries" (i.e., the costs and burdens of avoiding the feared surveillance) could not be traced to any provable government activity. *Id.* at 1150-53.[33] That is not the case here.

---

[33] I note in passing one significant difference between the metadata collection at issue in this case and the electronic surveillance at issue in *Clapper.* As the Court noted in *Clapper,* "if the Government intends to use or disclose information obtained or derived from a [50 U.S.C.] § 1881a acquisition in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the

(Continued on following page)

The NSA's Bulk Telephony Metadata Program involves two potential searches: (1) the bulk collection of metadata and (2) the analysis of that data through the NSA's querying process. For the following reasons, I have concluded that the plaintiffs have standing to challenge both. First, as to the collection, the Supreme Court decided *Clapper* just months *before* the June 2013 news reports revealed the existence and scope of certain NSA surveillance activities. Thus, whereas the plaintiffs in *Clapper* could only speculate as to whether they would be surveilled at all, plaintiffs in this case can point to strong evidence that, as Verizon customers, their telephony metadata has been collected for the last seven years (and stored for the last five) and will continue to be collected barring judicial or legislative intervention. *Compare id.* at 1148 ("[R]espondents have no actual knowledge of the Government's § 1881a targeting practices."), *with* Pls.' Mem. at 1, 2 n.2, 7-8 (citing FISC orders and statements from Director of National Intelligence); Suppl. Klayman Aff. ¶ 3 (attesting to status as Verizon customer); Strange Aff. ¶ 2 (same). In addition, the Government has declassified and authenticated an April

---

lawfulness of the acquisition." 133 S. Ct. at 1154 (citing 50 U.S.C. §§ 1806(c), 1806(e), 1881e(a)). Sections 1806(c) and (e) and 1881e(a), however, apply only to "information obtained or derived from an electronic surveillance" authorized by specific statutes; they do *not* apply to business records collected under Section 1861. Nor does it appear that any other statute requires the Government to notify a criminal defendant if it intends to use evidence derived from an analysis of the bulk telephony metadata collection.

25, 2013 FISC Order signed by Judge Vinson, which confirms that the NSA has indeed collected telephony metadata from Verizon. *See* Apr. 25, 2013 Secondary Order.

Straining mightily to find a reason that plaintiffs nonetheless lack standing to challenge the metadata collection, the Government argues that Judge Vinson's order names only Verizon Business Network Services ("VBNS") as the recipient of the order, whereas plaintiffs claim to be Verizon Wireless subscribers. *See* Govt's Opp'n at 21 & n.9. The Government obviously wants me to infer that the NSA may not have collected records from Verizon Wireless (or perhaps any other non-VBNS entity, such as AT & T and Sprint). Curiously, the Government makes this argument at the same time it is describing in its pleadings a bulk metadata collection program that can function *only* because it "creates an historical repository that permits retrospective analysis of terrorist-related communications *across multiple telecommunications networks,* and that can be immediately accessed as new terrorist-associated telephone identifiers come to light." Govt's Opp'n at 12 (emphasis added); *see also id.* at 65 (court orders to segregate and destroy individual litigants' records "could ultimately have a degrading effect on the utility of the program"); Shea Decl. ¶ 65 (removing plaintiffs' phone numbers "could undermine the results of any authorized query of a phone number that based on RAS is associated with one of the identified foreign terrorist organizations by eliminating, or cutting off potential call chains").

Put simply, the Government wants it both ways. Virtually all of the Government's briefs and arguments to this Court explain how the Government has acted in good faith to create a *comprehensive* metadata database that serves as a potentially valuable tool in combating terrorism – in which case, the NSA *must* have collected metadata from Verizon Wireless, the single largest wireless carrier in the United States, as well as AT & T and Sprint, the second and third-largest carriers. *See Grading the top U.S. carriers in the third quarter of 2013,* FIERCEWIRELESS.COM (Nov. 18, 2013);[34] Marguerite Reardon, *Competitive wireless carriers take on AT & T and Verizon,* CNET.COM (Sept. 10, 2012).[35] Yet in one footnote, the Government asks me to find that plaintiffs lack standing based on the theoretical possibility that the NSA has collected a universe of metadata so incomplete that the program could not possibly serve its putative function.[36] Candor of this type defies common sense and does not exactly inspire confidence!

---

[34] http://www.fiercewireless.com/special-reports/grading-top-us-carriers-third-quarter-2013.

[35] http://news.cnet.com/8301-1035_3-57505803-94/competitive-wireless-carriers-take-on-at-t-and-verizon/.

[36] To draw an analogy, if the NSA's program operates the way the Government suggests it does, then omitting Verizon Wireless, AT&T, and Sprint from the collection would be like omitting John, Paul, and George from a historical analysis of the Beatles. A Ringo-only database doesn't make any sense, and I cannot believe the Government would create, maintain, and so ardently defend such a system.

Likewise, I find that plaintiffs also have standing to challenge the NSA's querying procedures, though not for the reasons they pressed at the preliminary injunction hearing. At oral argument, I specifically asked Mr. Klayman whether plaintiffs had any "basis to believe that the NSA has done any queries" involving their phone numbers. Transcript of Nov. 18, 2013 Preliminary Injunction Hearing at 22, *Klayman I* & *Klayman II* ("P.I. Hr'g Tr.") [Dkt. # 41]. Mr. Klayman responded: "I think they are messing with me." *Id.* He then went on to explain that he and his clients had received inexplicable text messages and emails, not to mention a disk containing a spyware program. *Id.*; *see also* Strange Aff. ¶¶ 12-17. Unfortunately for plaintiffs, none of these unusual occurrences or instances of being "messed with" have anything to do with the question of whether the NSA has ever queried or analyzed their telephony metadata, so they do not confer standing on plaintiffs.

The Government, however, describes the advantages of bulk collection in such a way as to convince me that plaintiffs' metadata – indeed *everyone's* metadata – is analyzed, manually or automatically,[37] whenever the Government runs a query using as the "seed" a phone number or identifier associated with a phone for which the NSA has not collected metadata

[37] *See* Oct. 11, 2013 Primary order at 11 ("Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below."); *see also supra* note 22.

(e.g., phones operating through foreign phone companies). According to the declaration submitted by NSA Director of Signals Intelligence Directorate ("SID") Teresa H. Shea, the data collected as part of the Bulk Telephony Metadata Program – had it been in place at that time – would have allowed the NSA to determine that a September 11 hijacker living in the United States had contacted a known al Qaeda safe house in Yemen. Shea Decl. ¶ 11. Presumably, the NSA is not collecting metadata from whatever Yemeni telephone company was servicing that safehouse, which means that the metadata program remedies the investigative problem in Director Shea's example *only if* the metadata can be queried to determine which callers in the United States had ever contacted or been contacted by the target Yemeni safehouse number. *See also* Shea Decl. ¶ 44 (the metadata collection allows NSA analysts to, among other things, "detect foreign identifiers associated with a foreign terrorist organization calling into the U.S. and discover which domestic identifiers are in contact with the foreign identifiers."). When the NSA runs such a query, its system must necessarily analyze metadata for *every* phone number in the database by comparing the foreign target number against *all* of the stored call records to determine which U.S. phones, if any, have interacted with the target number.[38] Moreover,

[38] The difference between querying a phone number belonging to a domestic Verizon subscriber (for which metadata has been collected) and querying a foreign number (for which metadata has not been collected) might be analogized as follows. A

(Continued on following page)

unlike a DNA or fingerprint database – which contains only a single "snapshot" record of each person therein – the NSA's database is updated every single day with new information about each phone number. *Compare Johnson v. Quander,* 440 F.3d 489, 498-99 (D.C. Cir. 2006), *with* Govt's Opp'n at 8-9. Because the Government can use daily metadata collection to engage in "repetitive, surreptitious surveillance of a citizen's private goings on," the NSA database "implicates the Fourth Amendment each time a government official monitors it."[39] (distinguishing DNA profile in a law enforcement database – which is not searched each time database is accessed – from a "constantly updat[ing]" video feed, and warning that

---

query that begins with a domestic U.S. phone number is like entering a library and looking to find all of the sources that are cited in *Battle Cry of Freedom* by James M. McPherson (Oxford University Press 1988). You find that specific book, open it, and there they are. "Hop one" is complete. Then, you want to find all the sources cited within each of those sources ("hop two"), and so on. At the end of a very long day, you have looked only at books, articles, etc. that were linked to *Battle Cry of Freedom.*

Querying a foreign phone number is like entering a library and trying to find every book that cites *Battle Cry of Freedom* as a source. It might be referenced in a thousand books. It might be in just ten. It could be in zero. The only way to know is to check every book. At the end of a very long month, you are left with the "hop one" results (those books that cite *Battle Cry of Freedom*), but to get there, you had to open every book in the library.

[39] It is irrelevant for Fourth Amendment purposes that the NSA might sometimes use automated analytical software. *Cf. Smith,* 442 U.S. at 744-45 ("We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.").

"future technological advances in DNA testing . . . may empower the government to conduct wide-ranging 'DNA dragnets' that raise justifiable citations to George Orwell"). And the NSA can access its database whenever it wants, repeatedly querying any seed approved in the last 180 days (for terms believed to be used by U.S. persons) or year (for all other terms). *See* Oct. 11, 2013 Primary Order at 10.[40]

---

[40] The Government contends that "the mere collection of Plaintiffs' telephony metadata . . . without review of the data pursuant to a query" cannot be considered a search "because the Government's acquisition of an item without examining its contents 'does not compromise the interest in preserving the privacy of its contents.'" Govt.'s Opp'n at 49 n.33 (quoting *Horton v. California,* 496 U.S. 128, 141 n.11 (1990); citing *United States v. Van Leeuwen,* 397 U.S. 249, 252-53 (1970)). The cases on which the Government relies are inapposite. *Horton* involved the seizure of tangible items under the plain view doctrine. 496 U.S. at 141-42. The Government quotes dicta about whether the seizure of a physical container constitutes a search of the container's contents. *Id.* at 141 n.11. Likewise, the Court in *Van Leeuwen* addressed whether the detention of a package constituted an unreasonable seizure. 397 U.S. at 252-53.

In the case of the bulk telephony metadata collection, there is no analogous "container" that remains sealed; rather, all of the metadata is handled by the Government, *at least* to the degree needed to integrate the metadata into the NSA's database. *See* Shea Decl. ¶¶ 17, 60 (government may access metadata for purpose of "rendering [it] useable to query" because "each [telecom] provider may not maintain records in a format that is subject to a standardized query"). Thus, unlike the contents of the container described in *Horton,* telephony metadata is not kept in an unmolested, opaque package that obscures it from the Government's view.

Accordingly, plaintiffs meet the standing requirements set forth in *Clapper,* as they can demonstrate that the NSA has collected and analyzed their telephony metadata and will continue to operate the program consistent with FISC opinions and orders. Whether doing so violates plaintiffs' Fourth Amendment rights is, of course, a separate question and the subject of the next section, which addresses the merits of their claims. *See United States v. Lawson,* 410 F.3d 735, 740 n.4 (D.C. Cir. 2005) ("[A]lthough courts sometimes refer to the reasonable expectation of privacy issue as 'standing' to contest a search, the question 'is more properly placed within the purview of substantive Fourth Amendment law than within that of standing.'" (quoting *Minnesota v. Carter,* 525 U.S. 83, 88 (1998)).

b. Plaintiffs Are Likely to Succeed on the Merits of Their Fourth Amendment Claim.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend IV. That right "shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id. A* Fourth Amendment "search" occurs either when "the Government obtains information by physically intruding on a constitutionally protected area," *United States v.*

Jones, 132 S. Ct. 945, 950 n.3 (2012), or when "the government violates a subjective expectation of privacy that society recognizes as reasonable," *Kyllo v. United States,* 533 U.S. 27, 33 (2001) (citing *Katz v. United States,* 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). This case obviously does not involve a physical intrusion, and plaintiffs do not claim otherwise.[41]

The threshold issue that I must address, then, is whether plaintiffs have a reasonable expectation of privacy that is violated when the Government indiscriminately collects their telephony metadata along with the metadata of hundreds of millions of other citizens without any particularized suspicion of wrongdoing, retains all of that metadata for five years, and then queries, analyzes, and investigates that data without prior judicial approval of the investigative targets. If they do – and a Fourth Amendment search has thus occurred – then the next step of the analysis will be to determine whether such a search is "reasonable." *See id.* at 31 (whether a search has occurred

[41] "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen,* 466 U.S. 109, 113 (1984). Plaintiffs have not offered any theory as to how they would have a possessory interest in their phone data held by Verizon, and I am aware of none.

is an "antecedent question" to whether a search was reasonable).[42]

i. The Collection and Analysis of Telephony Metadata Constitutes a Search.

The analysis of this threshold issue of the expectation of privacy must start with the Supreme Court's landmark opinion in *Smith v. Maryland,* 442 U.S. 735 (1979), which the FISC has said "squarely control[s]" when it comes to "[t]he production of telephone service provider metadata." Am. Mem. Op., *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from [REDACTED],* No. BR 13-109 at 6-9 (FISC Aug. 29, 2013) (attached as Ex. A to Gilligan Decl.) [Dkt. # 25-2]. In *Smith,* police were investigating a robbery victim's reports that she had received threatening and obscene phone calls from someone claiming to be the robber. *Id.* at 737. Without obtaining a warrant or court order, police installed a pen register, which revealed that a telephone in Smith's home had been used to call the

[42] While it is true "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear," *City of Ontario v. Quon,* 130 S. Ct. 2619, 2629 (2010), phone call and text messaging technology is not "emerging," nor is "its role in society" unclear. I therefore believe that it is appropriate and necessary to elaborate on the Fourth Amendment implications of the NSA's metadata collection program.

victim on one occasion.[43] The Supreme Court held that Smith had no reasonable expectation of privacy in the numbers dialed from his phone because he voluntarily transmitted them to his phone company, and because it is generally known that phone companies keep such information in their business records. *Id.* at 742-44. The main thrust of the Government's argument here is that under *Smith,* no one has an expectation of privacy, let alone a reasonable one, in the telephony metadata that telecom companies hold as business records; therefore, the Bulk Telephony Metadata Program is not a search. Govt's Opp'n at 45-50. I disagree.

The question before me is *not* the same question that the Supreme Court confronted in *Smith.* To say the least, "whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment," *id.* at 736 – under the circumstances addressed and contemplated in that case – is a far cry from the issue in this case.

Indeed, the question in this case can more properly be styled as follows: When do present-day circumstances – the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies

---

[43] A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted" (i.e., it records limited data on outgoing calls). 18 U.S.C. § 3127(3).

– become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.

In *United States v. Jones,* 132 S. Ct. 945 (2012), five justices found that law enforcement's use of a GPS device to track a vehicle's movements for nearly a month violated Jones's reasonable expectation of privacy. *See id.* at 955-56 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring). Significantly, the justices did so *without* questioning the validity of the Court's earlier decision in *United States v. Knotts,* 460 U.S. 276 (1983), that use of a tracking beeper does not constitute a search because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[44] *Id.* at 281. Instead, they emphasized the many significant ways in which the short-range, short-term tracking device used in *Knotts* differed from the constant month-long surveillance achieved with the GPS device attached to Jones's car. *See Jones,* 132 S. Ct. at 956 n.* (Sotomayor, J., concurring) (*Knotts* "does not foreclose

[44] In *Jones,* the Government relied heavily on *Knotts* (and *Smith*) as support for the argument that Jones had no expectation of privacy in his movements on the roads because he voluntarily disclosed them to the public. *See generally* Brief for Petitioner, *United States v. Jones,* 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 3561881; Reply Brief for Petitioner, *United States v. Jones,* 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 5094951. Five justices found that argument unconvincing.

the conclusion that GPS monitoring, in the absence of a physical intrusion, is a Fourth Amendment search"); *id.* at 964 (Alito, J., concurring) ("[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." (citation omitted)); *see also United States v. Maynard,* 615 F.3d 544, 557 (D.C. Cir. 2010), *aff'd sub nom. Jones,* 132 S. Ct. 945 ("*Knotts* held only that '[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,' not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end, as the Government would have it." (citation omitted; quoting *Knotts,* 460 U.S. at 281)).[45]

Just as the Court in *Knotts* did not address the kind of surveillance used to track Jones, the Court in *Smith* was not confronted with the NSA's Bulk

[45] Lower courts, too, have recognized that the Supreme Court's Fourth Amendment decisions cannot be read too broadly. *See, e.g., United States v. Cuevas-Sanchez,* 821 F.2d 248, 251 (5th Cir. 1987) ("It does not follow that [*California v. Ciraolo*, 476 U.S. 207 (1986), which held that police did not violate a reasonable expectation of privacy when they engaged in a warrantless aerial observation of marijuana plants growing on curtilage of a home using only the naked eye from a height of 1,000 feet,] authorizes any type of surveillance whatever just because one type of minimally-intrusive aerial observation is possible.").

Telephony Metadata Program.[46] Nor could the Court in 1979 have ever imagined how the citizens of 2013 would interact with their phones. For the many reasons discussed below, I am convinced that the surveillance program now before me is so different from a simple pen register that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search. To the contrary, for the following reasons, I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.

First, the pen register in *Smith* was operational for only a matter of days between March 6, 1976 and March 19, 1976, and there is no indication from the

---

[46] True, the Court in *Knotts* explicitly "reserved the question whether 'different constitutional principles may be applicable' to 'dragnet-type law enforcement practices' of the type that GPS tracking made possible" in *Jones*. *Jones,* 132 S. Ct. at 952 n.6 (quoting *Knotts,* 460 U.S. at 284); *see also id.* at 956, n.* (Sotomayor, J., concurring). That the Court in *Smith* did not explicitly hold open the question of whether an exponentially broader, high-tech, years-long bulk telephony metadata collection program would infringe on reasonable expectations of privacy does not mean that the Court's holding necessarily extends so far as to answer that novel question. The Supreme Court itself has recognized that prior Fourth Amendment precedents and doctrines do not always control in cases involving unique factual circumstances created by evolving technology. *See, e.g., Kyllo,* 533 U.S. at 34 ("To withdraw protection of this minimum expectation [of privacy in the home] would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."). If this isn't such a case, then what is?

Court's opinion that it expected the Government to retain those limited phone records once the case was over. *See* 442 U.S. at 737. In his affidavit, Acting Assistant Director of the FBI Robert J. Holley himself noted that "[p]en-register and trap-and-trace (PR/TT) devices provide no historical contact information, only a record of contacts with the target occurring after the devices have been installed." Holley Decl. ¶ 9. This short-term, forward-looking (as opposed to historical), and highly-limited data collection is what the Supreme Court was assessing in *Smith.* The NSA telephony metadata program, on the other hand, involves the creation and maintenance of a historical database containing *five years'* worth of data. And I might add, there is the very real prospect that the program will go on for as long as America is combatting terrorism, which realistically could be forever!

Second, the relationship between the police and the phone company in *Smith* is *nothing* compared to the relationship that has apparently evolved over the last seven years between the Government and telecom companies. *Compare Smith,* 442 U.S. at 737 ("[T]he telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at petitioner's home."), *with* Govt's Opp'n at 8-9 ("Under this program, . . . certain telecommunications service providers [] produce to the NSA *on a daily basis* electronic copies of call detail records, or telephony metadata. . . . The FISC *first authorized the program in May 2006,* and since then has renewed the program thirty-five

times. . . ." (emphases added; citation and internal quotation marks omitted)). The Supreme Court itself has long-recognized a meaningful difference between cases in which a third party collects information and then turns it over to law enforcement, *see, e.g., Smith,* 442 U.S. 735; *United States v. Miller,* 425 U.S. 435 (1976), and cases in which the government and the third party create a formalized policy under which the service provider collects information for law enforcement purposes, *see Ferguson v. Charleston,* 532 U.S. 67 (2001), with the latter raising Fourth Amendment concerns. In *Smith,* the Court considered a one-time, targeted request for data regarding an individual suspect in a criminal investigation, *see Smith,* 442 U.S. at 737, which in no way resembles the daily, all-encompassing, indiscriminate dump of phone metadata that the NSA now receives as part of its Bulk Telephony Metadata Program. It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation with the Government. *Cf. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press,* 489 U.S. 749, 764 (1989) ("Plainly there is a vast difference between the public records that might be found after a diligent search of [various third parties' records] and a computerized

summary located in a single clearinghouse of information.").[47]

Third, the almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979. In *Smith,* the Supreme Court was actually considering whether local police could collect one person's phone records for calls made after the pen register was installed and for the limited purpose of a small-scale investigation of harassing phone calls. *See Smith,* 442 U.S. at 737. The notion that the Government could collect similar data on hundreds of millions of people and retain that data for a five-year period, updating it with new data every day in perpetuity, was at best, in 1979, the stuff of science fiction. By comparison, the Government has at its disposal today the most advanced twenty-first century tools, allowing it to "store such records and efficiently mine them for information years into the future." *Jones,* 132 S. Ct. at 956 (Sotomayor, J., concurring). And

[47] When an individual makes his property accessible to third parties, he may still retain some expectation of privacy based on his understanding of how third parties typically handle that property. *See Bond v. United States,* 529 U.S. 334, 338-39 (2000) ("[A] bus passenger clearly expects that his bag may be handled. He does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner. But this is exactly what the agent did here. We therefore hold that the agent's physical manipulation of petitioner's bag violated the Fourth Amendment.").

these technologies are "cheap in comparison to conventional surveillance techniques and, by design, proceed[ ] surreptitiously," thereby "evad[ing] the ordinary checks that constrain abusive law enforcement practices: limited police . . . resources and community hostility." *Id.*[48]

Finally, *and most importantly,* not only is the Government's ability to collect, store, and analyze phone data greater now than it was in 1979, but the nature and quantity of the information contained in people's telephony metadata is much greater, as well. According to the 1979 U.S. Census, in that year, 71,958,000 homes had telephones available, while 6,614,000 did not. U.S. DEP'T OF COMMERCE & U.S. DEP'T OF HOUS. & URBAN DEV., ANNUAL HOUSING SURVEY: 1979, at 4 (1981) (Table A-1: Characteristics of the Housing Inventory: 1979 and 1970). In December 2012, there were a whopping 326,475,248 mobile subscriber connections in the United States, of which approximately 304 million were for phones and twenty-two million were for computers, tablets, and

[48] The unprecedented scope and technological sophistication of the NSA's program distinguish it not only from the *Smith* pen register, but also from metadata collections performed as part of routine criminal investigations. To be clear, this opinion is focusing only on the program before me and not any other law enforcement practices. Like the concurring justices in *Jones,* I cannot "identify with precision the point at which" bulk metadata collection becomes a search, but there is a substantial likelihood that the line was crossed under the circumstances presented in this case. *See Jones,* 132 S. Ct. at 964 (Alito, J., concurring).

modems.[49] CTIA – The Wireless Ass'n ("CTIA"), *Wireless Industry Survey Results – December 1985 to December 2012,* at 2, 6 (2013) ("CTIA *Survey Results*");[50] *see also* Sixteenth Report, *In re Implementation of Section 6002(b) of Omnibus Budget Reconciliation Act,* WT Dkt. No. 11-186, at 9 (F.C.C. Mar. 21, 2013) ("[A]t the end of 2011 there were 298.3 million subscribers to mobile telephone, or voice, service, up nearly 4.6 percent from 285.1 million at the end of 2010."). The number of mobile subscribers in 2013 is more than *3,000 times* greater than the 91,600 subscriber connections in 1984, INDUS. ANALYSIS DIV., FED. COMMC'NS COMM'N, TRENDS IN TELEPHONE SERVICE 8 (1998), and more than *triple* the 97,035,925 subscribers in June 2000, CTI *Survey Results, supra,* at 4.[51] It is now safe to assume that the vast majority of people reading this opinion have *at least* one cell phone within arm's reach (in addition to other mobile devices). Joanna Brenner, *Pew Internet: Mobile* (Sept. 18, 2013) (91% of American adults have a cell phone,

---

[49] The global total is 6.6 billion. Ericsson, *Mobility Report on the Pulse of Networked Society,* at 4 (Nov. 2013), *available at* http://www.ericsson.com/res/docs/2013/ericsson-mobility-report november-2013.pdf.

[50] http://files.ctia.org/pdf/CTIA_Survey_YE_2012_Graphics-FINAL.pdf.

[51] Mobile phones are rapidly replacing traditional landlines, with 38.2% of households going "wireless-only" in 2012. CTIA, *Wireless Quick Facts,* http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts (last visited Dec. 10, 2013); *see also* Jeffrey Sparshott, *More People Say Goodbye to Landlines,* Wall St. J., Sept. 6, 2013, at A5.

95-97% of adults age 18 to 49);[52] CTIA, *Wireless Quick Facts* (last visited Dec. 10, 2013) ("CTIA *Quick Facts*") (wireless penetration – the number of active wireless units divided by total U.S. and territorial population – was 102.2% as of December 2012).[53] In fact, some undoubtedly will be reading this opinion *on their cell phones.* Maeve Duggan, *Cell Phone Activities 2013* (Sept. 19, 2013) (60% of cell phone owners use them to access internet).[54] Cell phones have also morphed into multi-purpose devices. They are now maps and music players. *Id.* (49% of cell phone owners use their phones to get directions and 48% to listen to music). They are cameras. Keith L. Alexander, *Camera phones become courthouse safety issue,* WASH. POST, Apr. 22, 2013, at B01. They are even lighters that people hold up at rock concerts. Andy Rathbun, *Cool 2 Know – Cellphone virtuosos,* NEWSDAY, Apr. 20, 2005, at B02. They are ubiquitous as well. Count the phones at the bus stop, in a restaurant, or around the table at a work meeting or any given occasion. Thirty-four years ago, *none* of those phones would have been there.[55] Thirty-four years ago, city streets were lined

---

[52] http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx.

[53] http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts.

[54] http://pewinternet.org/Reports/2013/Cell-Activities/Main-Findings.aspx.

[55] *Mobile Telephone,* BRITANNICA.COM, http://www.britannica.com/EBchecked/topic/1482373/mobile-telephone?anchor=ref1079017 (last visited Dec. 13, 2013) ("[A] Japanese system was the first

(Continued on following page)

with pay phones. Thirty-four years ago, when people wanted to send "text messages," they wrote letters and attached postage stamps.[56]

Admittedly, what metadata *is* has not changed over time. As in *Smith,* the *types* of information at issue in this case are relatively limited: phone numbers dialed, date, time, and the like.[57] But the

---

cellular system to be deployed, in 1979."); Tom Farley, *Mobile telephone history,* TELEKTRONIKK, March/April 2005, at 28 ("An 88 cell system in the challenging cityscape of Tokyo began in December, 1979. . . . The first North American commercial system began in August, 1981 in Mexico City.").

[56] It is not clear from the pleadings whether "telephony metadata" and "comprehensive communications routing information" includes data relating to text messages. *See supra* note 16. If it does, then in 2012, the Government collected an additional *six billion* communications *each day* (69,635 *each second*). *See* Infographic – *Americans sent and received more than 69,000 texts every second in 2012,* CTIA.org (Nov. 25, 2013), http://www.ctia.org/resourcelibrary/facts-and-infographics/archive/americans-texts-2012-infographic.

[57] There are, however, a few noteworthy distinctions between the data at issue in *Smith* and the metadata that exists nowadays. For instance, the pen register in *Smith* did not tell the government whether calls were completed or the duration of any calls, *see Smith,* 442 U.S. at 741, whereas that information is captured in the NSA's metadata collection.

A much more significant difference is that telephony metadata can reveal the user's location, *see generally New Jersey v. Earls,* 70 A.3d 630, 637-38 (N.J. 2013), which in 1979 would have been entirely unnecessary given that landline phones are tethered to buildings. The most recent FISC order explicitly "does not authorize the production of cell site location information," Oct. 11, 2013 Primary order at 3 n. 1, and the Government has publicly disavowed such collection, *see* Transcript of

(Continued on following page)

June 25, 2013 Newseum Special Program: NSA Surveillance Leaks: Facts and Fiction, Remarks of Robert Litt, Gen. Counsel, Office of Dir. of Nat'l Intelligence, *available at* http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-and-fiction ("I want to make perfectly clear we do not collect cellphone location information under this program, either GPS information or cell site tower information.").

That said, not all FISC orders have been made public, and I have no idea how location data has been handled in the past. Plaintiffs *do* allege that location data has been collected, *see* Second Am. Compl. ¶ 28; Pls.' Mem. at 10-11, and the Government's brief does not refute that allegation (though one of its declarations does, *see* Shea Decl. ¶ 15). *See also supra* note 17. Moreover, the most recent FISC order states, and defendants concede, that " 'telephony metadata' includes . . . trunk identifier[s]," Oct. 11, 2013 Primary order at 3 n.1; Govt's Opp'n at 9, which apparently "can reveal where [each] call enter[s] the trunk system" and can be used to "locate a phone within approximately a square kilometer," Patrick Di Justo, *What the N.S.A. Wants to Know About Your Calls,* NEW YORKER (June 7, 2013), http://www.newyorker.com/online/blogs/elements/2013/06/what-the-nsa-wants-to-know-about-your-phone-calls.html. And "if [the metadata] includes a request for every trunk identifier used throughout the interaction," that "could allow a phone's movements to be tracked." *Id.* Recent news reports, though not confirmed by the Government, cause me to wonder whether the Government's briefs are entirely forthcoming about the full scope of the Bulk Telephony Metadata Program. *See, e.g.,* Barton Gellman & Ashkan Soltani, *NSA maps targets by their phones,* WASH. POST, Dec. 5, 2013, at A01.

The collection of location data would, of course, raise its own Fourth Amendment concerns, *see, e.g., In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't,* 620 F.3d 304, 317 (3d Cir. 2010) ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful

(Continued on following page)

ubiquity of phones has dramatically altered the *quantity* of information that is now available and, *more importantly,* what that information can tell the Government about people's lives. *See Quon,* 130 S. Ct. at 2630 ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. . . . [And] the ubiquity of those devices has made them generally affordable. . . ."); *cf. Jones,* 132 S. Ct. at 956 (Sotomayor, J., concurring) (discussing the "substantial quantum of intimate information about any person" captured by GPS tracking). Put simply, people in 2013 have an entirely different relationship with phones than they did thirty-four years ago. As a result, people make calls and send text messages now that they would not (really, *could not*) have made or sent back when *Smith* was decided – for example, every phone call today between two people trying to locate one another in a public place. *See* CTIA *Quick Facts, supra* (2.3 *trillion* voice minutes used in 2012, up from 62.9 billion in 1997). This rapid and monumental shift towards a cell phone-centric culture means that the metadata from each person's phone "reflects a wealth of detail about her familial,

---

way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information."), but my decision on this preliminary injunction does *not* turn on whether the NSA has in fact collected that data as part of the bulk telephony metadata program.

political, professional, religious, and sexual associations," *Jones,* 132 S. Ct. at 955 (Sotomayor, J., concurring), that could not have been gleaned from a data collection in 1979. *See also* Decl. of Prof. Edward W. Felten ("Felten Decl.") [Dkt. # 22-1], at ¶¶ 38-58. Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic – a vibrant and constantly updating picture of the person's life. *See Maynard,* 615 F.3d at 562-63.[58] Whereas some may assume that these cultural changes will force people to "reconcile themselves" to an "inevitable" "diminution of privacy that new technology entails," *Jones,* 132 S. Ct. at 962

[58] The Government maintains that the metadata the NSA collects does not contain personal identifying information associated with each phone number, and in order to get that information the FBI must issue a national security letter ("NSL") to the phone company. Govt's Opp'n at 48-49; P.I. Hr'g Tr. at 44-45. Of course, NSLs do not require *any* judicial oversight, *see* 18 U.S.C. § 2709; 12 U.S.C. § 3414, 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 50 U.S.C. § 3162, meaning they are hardly a check on potential abuses of the metadata collection. There is also nothing stopping the Government from skipping the NSL step altogether and using public databases or any of its other vast resources to match phone numbers with subscribers. *See, e.g.,* James Ball et al., *Covert surveillance: The reaction: 'They are tracking the calling patterns of the entire country',* GUARDIAN, June 7, 2013, at 5 ("[W]hen cross-checked against other public records, the metadata can reveal someone's name, address, driver's licence, credit history, social security number and more."); Felten Decl. ¶ 19 & n.14; Suppl. Decl. of Prof. Edward W. Felten [Dkt. # 28], at ¶¶ 3-4 ("[I]t would be trivial for the government to obtain a subscriber's name once it has that subscriber's phone number. . . . It is extraordinarily easy to correlate a phone number with its unique owner.").

(Alito, J., concurring), I think it is more likely that these trends have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable.[59]

In sum, the *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones. Plaintiffs have alleged that they engage in conduct that exhibits a subjective expectation of privacy in the bulk, five-year historical record of their telephony metadata, *see* Pls.' Mem. at 21; Suppl. Klayman Aff. ¶¶ 5, 10, 13; Strange Aff. ¶¶ 11, 19, and I have no reason to question the genuineness of those subjective beliefs.[60] The more difficult

---

[59] Public opinion polls bear this out. *See, e.g.,* Associated Press, *9/11 Anniversary: Poll finds public doubts growing on federal surveillance, privacy,* Hous. Chron., Sept. 11, 2013, at A6 ("Some 56 percent oppose the NSA's collection of telephone records for future investigations even though they do not include actual conversations.").

[60] If plaintiffs *lacked* such a subjective expectation of privacy in all of their cell phone metadata, I would likely find that it is the result of "'condition[ing]' by influences alien to well-recognized Fourth Amendment freedoms." *Smith,* 442 U.S. at 740 n.5. In 1979, the Court announced that numbers dialed on a phone are not private, and since that time, the Government and courts have gradually (but significantly) expanded the scope of what that holding allows. Now, even local police departments are routinely requesting and obtaining massive cell phone "tower dumps," each of which can capture data associated with thousands of innocent Americans' phones. *See* Ellen Nakashima, *'Tower*

(Continued on following page)

question, however, is whether their expectation of privacy is one that society is prepared to recognize as objectively reasonable arid justifiable. As I said at the outset, the question before me is not whether *Smith* answers the question of whether people can have a reasonable expectation of privacy in telephony metadata under all circumstances. Rather, the question that I will ultimately have to answer when I reach the merits of this case someday is whether people have a reasonable expectation of privacy that is violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-tech querying and analysis without any case-by-case judicial approval. For the many reasons set forth above,

---

dumps' give police masses of cellphone data, Wash. Post, Dec. 9, 2013, at A01 Targeted tower dumps may be appropriate under certain circumstances and with appropriate oversight and limitations, *see In re Search of Cellular Tel. Towers,* ___ F. Supp. 2d ___, 2013 WL 1932881, at *2 (S.D. Tex. May 8, 2013) (requiring warrant and return of all irrelevant records to telecom provider for 77-tower dump of all data for five-minute period), and fortunately, that question is not before me here. The point is, however, that the experiences of many Americans – especially those who have grown up in the post-*Smith,* post-cell phone, post-PATRIOT Act age – might well be compared to those of the "refugee from a totalitarian country, unaware of this Nation's traditions, [who] erroneously assume[ ] that police were continuously monitoring" telephony metadata. *Smith,* 442 U.S. at 740 n.5. Accordingly, their "subjective expectations obviously could play no meaningful role in ascertaining . . . the scope of Fourth Amendment protection," and "a normative inquiry would be proper." *Id.*

it is significantly likely that on that day, I will answer that question in plaintiffs' favor.

ii. There Is a Significant Likelihood Plaintiffs Will Succeed in Showing that the Searches Are Unreasonable.

Having found that a search occurred in this case, I next must "examin[e] the totality of the circumstances to determine whether [the] search is reasonable within the meaning of the Fourth Amendment." *Samson v. California,* 547 U.S. 843, 848 (2006) (internal quotation marks omitted). '"[A]s a general matter, warrantless searches are *per se* unreasonable under the Fourth Amendment.'" *Nat'l Fed'n of Fed. Emps.-IAM v. Vilsack,* 681 F.3d 483, 488-89 (D.C. Cir. 2012) (quoting *Quon,* 130 S. Ct. at 2630); *see also Chandler v. Miller,* 520 U.S. 305, 313 (1997) ("To be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing.").

The Supreme Court has recognized only a "'few specifically established and well-delineated exceptions to that general rule,'" *Nat'l Fed'n of Fed. Emps.-IAM,* 681 F.3d at 489 (quoting *Quon,* 130 S. Ct. at 2630), including one that applies when "'special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable,'" *id.* (quoting *Vernonia Sch. Dist. 47J v. Acton,* 515 U.S. 646, 653 (1995)). "Even where the

government claims 'special needs,'" as it does in this case, "a warrantless search is generally unreasonable unless based on 'some quantum of individualized suspicion.'" *Id.* (quoting *Skinner v. Ry. Labor Execs.' Ass'n,* 489 U.S. 602, 624 (1989)). Still, a suspicionless search may be reasonable "'where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion.'" *Id.* (quoting *Skinner,* 489 U.S. at 624). As such, my task is to "'balance the [plaintiffs'] privacy expectations against the government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context.'" *Id.* (quoting *Nat'l Treasury Emps. Union v. Von Raab,* 489 U.S. 656, 665-66 (1989)). This is a "'context-specific inquiry'" that involves "'examining closely the competing private and public interests advanced by the parties.'" *Id.* (quoting *Chandler,* 520 U.S. at 314)). The factors I must consider include: (1) "the nature of the privacy interest allegedly compromised" by the search, (2) "the character of the intrusion imposed" by the government, and (3) "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them." *Bd. of Educ. v. Earls,* 536 U.S. 822, 830-34 (2002).

"Special needs" cases, not surprisingly, form something of a patchwork quilt. For example, schools and government employers are permitted under certain circumstances to test students and employees for

drugs and alcohol, *see Earls,* 536 U.S. 822; *Vernonia Sch. Dist.,* 515 U.S. 646; *Von Raab,* 489 U.S. 656; *Skinner,* 489 U.S. 602, and officers may search probationers and parolees to ensure compliance with the rules of supervision, *see Griffin v. Wisconsin,* 483 U.S. 868 (1987).[61] The doctrine has also been applied in cases involving efforts to prevent acts of terrorism in crowded transportation centers. *See, e.g., Cassidy v. Chertoff,* 471 F.3d 67 (2d Cir. 2006) (upholding searches of carry-on bags and automobiles that passengers bring on ferries); *MacWade v. Kelly,* 460 F.3d 260 (2d Cir. 2006) (upholding searches of bags in New York City subway system). To my knowledge, however, no court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion. In effect, the Government urges me to be the first non-FISC judge to sanction such a dragnet.

For reasons I have already discussed at length, I find that plaintiffs have a very significant expectation of privacy in an aggregated collection of their

---

[61] Suspicionless searches and seizures have also been allowed in other contexts not analyzed under the "special needs" framework, including administrative inspections of "closely regulated" businesses, *see New York v. Burger,* 482 U.S. 691 (1987), searches of fire-damaged buildings for the purpose of determining the cause of the fire, *see Michigan v. Tyler,* 436 U.S. 499 (1978), and highway checkpoints set up to catch intoxicated motorists and illegal entrants into the United States, *see Mich. Dep't of State Police v. Sitz,* 496 U.S. 444 (1990); *United States v. Martinez-Fuerte,* 428 U.S. 543 (1976).

telephony metadata covering the last five years, and the NSA's Bulk Telephony Metadata Program significantly intrudes on that expectation.[62] Whether the program violates the Fourth Amendment will therefore turn on "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them." *Earls,* 536 U.S. at 834.

The Government asserts that the Bulk Telephony Metadata Program serves the "programmatic purpose"

---

[62] These privacy interests are not "mitigated . . . by the statutorily mandated restrictions on access to and dissemination of the metadata that are written into the FISC's orders." Govt's Opp'n at 51-52. First, there are no minimization procedures applicable at the collection stage; the Government acknowledges that FISC orders require the recipients to turn over all of their metadata without limit. *See* Oct. 11, 2013 Primary order at 3-4. Further, the most recent order of the FISC states that any trained NSA personnel can access the metadata, with "[t]echnical personnel" authorized to run queries even using non-RAS-approved selection terms for purposes of "perform[ing] those processes needed to make [the metadata] usable for intelligence analysis." *Id.* at 5. The "[r]esults of any intelligence analysis queries," meanwhile, "may be shared, *prior to minimization,* for intelligence analysis purposes among [trained] NSA analysts." *Id.* at 12-13 (emphasis added); *see also* Shea Decl. ¶¶ 30, 32 (minimization procedures "guard against inappropriate or unauthorized *dissemination* of information relating to U.S. persons," and "results of authorized queries of the metadata may be shared, *without minimization,* among trained NSA personnel for analysis purposes" (emphases added)). These procedures in no way mitigate the privacy intrusion that occurs when the NSA collects, queries, and analyzes metadata. And that's even *assuming* the Government complies with all of its procedures – an assumption that is not supported by the NSA's spotty track record to date. *See supra* notes 23-25 and accompanying text.

of "identifying unknown terrorist operatives and preventing terrorist attacks." Govt's Opp'n at 51 – an interest that everyone, including this Court, agrees is "of the highest order of magnitude," *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act,* 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008); *see also Haig v. Agee,* 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation." (internal quotation marks omitted)).[63] A closer examination of the record, however, reveals that the Government's interest is a bit more nuanced – it is not merely to investigate potential terrorists, but rather, to do so *faster* than other investigative methods might allow. Indeed, the affidavits in support of the Government's brief repeatedly emphasize this interest in speed. For example, according to SID Director Shea, the primary advantage of the bulk metadata collection is that "it enables the

[63] It bears noting that the Government's interest in stopping and prosecuting terrorism *has not* led courts to abandon familiar doctrines that apply in criminal cases generally. *See United States v. Ressam,* 679 F.3d 1069, 1106 (9th Cir. 2012) (Schroeder, J., dissenting) (collecting cases in which "courts have treated other issues in terrorism cases in ways that do not differ appreciably from more broadly applicable doctrines"). In fact, the Supreme Court once expressed in dicta that an otherwise impermissible roadblock "would *almost* certainly" be allowed "to thwart an *imminent* terrorist attack." *City of Indianapolis v. Edmond,* 531 U.S. 32, 44 (2000) (emphases added). The Supreme Court has never suggested that all Fourth Amendment protections must defer to any Government action that purportedly serves national security or counterterrorism interests.

Government to *quickly* analyze past connections and chains of communication," and "increases the NSA's ability to *rapidly* detect persons affiliated with the identified foreign terrorist organizations." Shea Decl. ¶ 46 (emphases added); *see also id.* ¶ 59 ("Any other means that might be used to attempt to conduct similar analyses would require *multiple, time-consuming steps* that would frustrate needed *rapid* analysis in emergent situations, and could fail to capture some data available through bulk metadata analysis." (emphases added)). FBI Acting Assistant Director of the Counterterrorism Division Robert J. Holley echoes Director Shea's emphasis on speed: "It is imperative that the United States Government have the capability to *rapidly* identify any terrorist threat inside the United States." Holley Decl. ¶ 4 (emphasis added); *see also id.* ¶¶ 28-29 ("[T]he *agility* of querying the metadata collected by NSA under this program allows for more *immediate* contact chaining, which is significant in *time-sensitive* situations. . . . The *delay* inherent in issuing new national security letters would necessarily mean losing *valuable time*. . . . [A]ggregating the NSA telephony metadata from different telecommunications providers enhances and *expedites* the ability to identify chains of communications across multiple providers." (emphases added)).

Yet, turning to the efficacy prong, the Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was

time-sensitive in nature. In fact, none of the three "recent episodes" cited by the Government that supposedly "illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack" involved any apparent urgency. *See* Holley Decl. ¶¶ 24-26. In the first example, the FBI learned of a terrorist plot still "in its early stages" and investigated that plot before turning to the metadata "to ensure that all potential connections were identified." *Id.* ¶ 24. Assistant Director Holley does not say that the metadata revealed any new information – much less time-sensitive information – that had not already come to light in the investigation up to that point. *Id.* In the second example, it appears that the metadata analysis was used only after the terrorist was arrested "to establish [his] foreign ties and put them in context with his U.S. based planning efforts." *Id.* ¶ 25. And in the third, the metadata analysis "revealed a previously unknown number for [a] co-conspirator . . . and corroborated his connection to [the target of the investigation] as well as to other U.S.-based extremists." *Id.* ¶ 26. Again, there is no indication that these revelations were immediately useful or that they prevented an impending attack. Assistant Director Holley even concedes that bulk metadata analysis only "*sometimes* provides information earlier than the FBI's other investigative methods and techniques." *Id.* ¶ 23 (emphasis added).[64] Given the limited record before me at this point in the

[64] Such candor is as refreshing as it is rare.

litigation – most notably, the utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics – I have serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.[65] *Chandler,* 520 U.S. at 318-19 ("Notably lacking in respondents' presentation is any indication of a concrete danger demanding departure from the Fourth Amendment's main rule."). Thus, plaintiffs have a substantial likelihood of showing that their privacy interests outweigh the Government's interest in collecting and analyzing bulk telephony metadata

---

[65] The Government could have requested permission to present additional, potentially classified evidence *in camera,* but it chose not to do so. Although the Government has publicly asserted that the NSA's surveillance programs have prevented fifty-four terrorist attacks, no proof of that has been put before me. *See also* Justin Elliott & Theodoric Meyer, *Claim on 'Attacks Thwarted' by NSA Spreads Despite Lack of Evidence,* ProPublica.org (Oct. 23, 2013), http://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence (" 'We've heard over and over again the assertion that 54 terrorist plots were thwarted' by the [NSA's] programs. . . . 'That's plainly wrong. . . . These weren't all plots and they weren't all thwarted. The American people are getting left with the inaccurate impression of the effectiveness of the NSA programs.' " (quoting Sen. Patrick Leahy)); Ellen Nakashima, *NSA's need to keep database questioned,* Wash. Post, Aug. 9, 2013, at A01 ("[Senator Ron] Wyden noted that [two suspects arrested after an investigation that involved use of the NSA's metadata database] were arrested 'months or years after they were first identified' by mining the phone logs.").

and therefore the NSA's bulk collection program is indeed an unreasonable search under the Fourth Amendment.[66]

I realize, of course, that such a holding might appear to conflict with other trial courts, *see, e.g., United States v. Moalin,* Crim. No. 10-4246, 2013 WL 6079518, at *5-8 (S.D. Cal. Nov. 18, 2013) (holding that bulk telephony metadata collection does not violate Fourth Amendment); *United States v. Graham,* 846 F. Supp. 2d 384, 390-405 (D. Md. 2012) (holding that defendants had no reasonable expectation of privacy in historical cell-site location information); *United States v. Gordon,* Crim. No. 09-153-02, 2012 WL 8499876, at *1-2 (D.D.C. Feb. 6, 2012) (same), and with longstanding doctrine that courts have applied in other contexts, *see, e.g., Smith,* 442 U.S. at 741-46 *Miller,* 425 U.S. at 443. Nevertheless, in reaching this decision, I find comfort in the statement in the Supreme Court's recent majority opinion in *Jones* that "[a]t bottom, we must 'assur[e] preservation of

---

[66] The Government points out that it could obtain plaintiffs' metadata through other means that potentially raise fewer Fourth Amendment concerns. *See* Govt's Opp'n at 6 ("The records must be of a type obtainable by either a grand jury subpoena, or an order issued by a U.S. court directing the production of records or tangible things." (citing 50 U.S.C. § 1861(c)(2)(D)); Holley Decl. ¶ 14 ("In theory, the FBI could seek a new set of orders on a daily basis for the records created within the preceding 24 hours."). Even if true, "[t]he fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment." *Kyllo,* 533 U.S. at 35 n.2.

that degree of privacy against government that existed when the Fourth Amendment was adopted.'" 132 S. Ct. at 950 (2012) (quoting *Kyllo,* 533 U.S. at 34). Indeed, as the Supreme Court noted more than a decade before *Smith,* "[t]he basic purpose of th[e Fourth] Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against *arbitrary invasions by governmental officials.*" *Camara v. Mun. Court,* 387 U.S. 523, 528 (1967) (emphasis added); *see also Quon,* 130 S. Ct. at 2627 ("The Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government, without regard to whether the government actor is investigating crime or performing another function." (internal quotation marks omitted)). The Fourth Amendment typically requires "a neutral and detached authority be interposed between the police and the public," and it is offended by "general warrants" and laws that allow searches to be conducted "indiscriminately and without regard to their connection with [a] crime under investigation." *Berger v. New York,* 388 U.S. 41, 54, 59 (1967). I cannot imagine a more "indiscriminate" and "arbitrary invasion" than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval. Surely, such a program infringes on "that degree of privacy" that the Founders enshrined in the Fourth Amendment. Indeed, I have little doubt that the author of our Constitution, James Madison, who cautioned us to

beware "the abridgement of freedom of the people by gradual and silent encroachments by those in power," would be aghast.[67]

2. Plaintiffs Will Suffer Irreparable Harm Absent Injunctive Relief

"It has long been established that the loss of constitutional freedoms, 'for even minimal periods of time, unquestionably constitutes irreparable injury.'" *Mills v. District of Columbia,* 571 F.3d 1304, 1312 (D.C. Cir. 2009) (quoting *Elrod v. Burns,* 427 U.S. 347, 373 (1976) (plurality opinion)). As in this case, the court in *Mills* was confronted with an alleged Fourth Amendment violation: a "Neighborhood Safety Zones" traffic checkpoint for vehicles entering a high-crime neighborhood in Washington, DC. *Id.* at 1306. After finding a strong likelihood of success on the merits, our Circuit Court had little to say on the irreparable injury prong, instead relying on the statement at the beginning of this paragraph that a constitutional violation, even of minimal duration, constitutes irreparable injury. Plaintiffs in this case

---

[67] James Madison, Speech in the Virginia Ratifying Convention on Control of the Military (June 16, 1788), *in* THE HISTORY OF THE VIRGINIA FEDERAL CONVENTION OF 1788, WITH SOME ACCOUNT OF EMINENT VIRGINIANS OF THAT ERA WHO WERE MEMBERS OF THE BODY (Vol. 1) 130 (Hugh Blair Grigsby et al. eds., 1890) ("Since the general civilization of mankind, I believe there are more instances of the abridgement of freedom of the people by gradual and silent encroachments by those in power than by violent and sudden usurpations.").

have also shown a strong likelihood of success on the merits of a Fourth Amendment claim. As such, they too have adequately demonstrated irreparable injury.

3. The Public Interest and Potential Injury to Other Interested Parties Also Weigh in Favor of Injunctive Relief.

"'[I]t is always in the public interest to prevent the violation of a party's constitutional rights.'" *Am. Freedom Def. Initiative v. Wash. Metro. Area Transit Auth.,* 898 F. Supp. 2d 73, 84 (D.D.C. 2012) (quoting *G & V Lounge, Inc. v. Mich. Liquor Control Comm'n,* 23 F.3d 1071, 1079 (6th Cir. 1994)); *see also Hobby Lobby Stores, Inc. v. Sebelius,* 723 F.3d 1114, 1145 (10th Cir. 2013) (same), *cert. granted,* ___ S. Ct. ___, 2013 WL 5297798 (2013); *Melendres v. Arpaio,* 695 F.3d 990, 1002 (9th Cir. 2012) (same); *Nat'l Fed'n of Fed. Emps. v. Carlucci,* 680 F. Supp. 416 (D.D.C. 1988) ("[T]he public interest lies in enjoining unconstitutional searches."). That interest looms large in this case, given the significant privacy interests at stake and the unprecedented scope of the NSA's collection and querying efforts, which likely violate the Fourth Amendment. Thus, the public interest weighs heavily in favor of granting an injunction.

The Government responds that the public's interest in combating terrorism is of paramount importance, *see* Govt's Opp'n at 64-65 – a proposition that I accept without question. But the Government offers no real explanation as to how granting relief

to these plaintiffs would be detrimental to that interest. Instead, the Government says that it will be burdensome to comply with any order that requires the NSA to remove plaintiffs from its database. *See id.* at 65; Shea Decl. ¶ 65. Of course, the public has no interest in saving the Government from the burdens of complying with the Constitution! Then, the Government frets that such an order "could ultimately have a degrading effect on the utility of the program if an injunction in this case precipitated successful requests for such relief by other litigants." Govt's Opp'n at 65 (citing Shea Decl. ¶ 65). For reasons already explained, I am not convinced at this point in the litigation that the NSA's database has ever truly served the purpose of rapidly identifying terrorists in time-sensitive investigations, and so I am *certainly* not convinced that the removal of two individuals from the database will "degrade" the program in any meaningful sense.[68] I will leave it to other judges to decide how to handle any future litigation in their courts.

---

[68] To the extent that removing plaintiffs from the database would create a risk of "eliminating, or cutting off potential call chains," Shea Decl. ¶ 65, the Government concedes that the odds of this happening are miniscule. *See* Govt's Opp'n at 2 ("[O]nly a tiny fraction of the collected metadata is ever reviewed. . . ."); Shea Decl. ¶ 23 ("Only the tiny fraction of the telephony metadata records that are responsive to queries authorized under the RAS standard are extracted, reviewed, or disseminated. . . .").

CONCLUSION

This case is yet the latest chapter in the Judiciary's continuing challenge to balance the national security interests of the United States with the individual liberties of our citizens. The Government, in its understandable zeal to protect our homeland, has crafted a counterterrorism program with respect to telephone metadata that strikes the balance based in large part on a thirty-four year old Supreme Court precedent, the relevance of which has been eclipsed by technological advances and a cell phone-centric lifestyle heretofore inconceivable. In the months ahead, other Article III courts, no doubt, will wrestle to find the proper balance consistent with our constitutional system. But in the meantime, for all the above reasons, I will grant Larry Klayman's and Charles Strange's requests for an injunction[69] and enter an order that (1) bars the Government from collecting, as part of the NSA's Bulk Telephony Metadata Program, any telephony metadata associated with their personal Verizon accounts and (2) requires the Government to destroy any such metadata in its possession that was collected through the bulk collection program.[70]

---

[69] For reasons stated at the outset, this relief is limited to *Klayman I* plaintiffs Larry Klayman and Charles Strange. I will deny Mary Ann Strange's motion and the motion in *Klayman II*.

[70] Although it is true that granting plaintiffs the relief they request will force the Government to identify plaintiffs' phone numbers and metadata records, and then subject them to

(Continued on following page)

However, in light of the significant national security interests at stake in this case and the novelty of the constitutional issues, I will stay my order pending appeal.[71] In doing so, I hereby give the Government fair notice that should my ruling be upheld, this order will go into effect forthwith. Accordingly, I fully expect that during the appellate process, which will consume at least the next six months, the Government will take whatever steps necessary to prepare itself to comply with this order when, and if, it is upheld. Suffice it to say, requesting further time to comply with this order months from now will not be well received and could result in collateral sanctions.

/s/ Richard J. Leon
RICHARD J. LEON
United States District Judge

---

otherwise unnecessary individual scrutiny, *see* Shea Decl. ¶ 64, that is the only way to remedy the constitutional violations that plaintiffs are substantially likely to prove on the merits.

[71] *See, e.g., Doe v. Gonzales,* 386 F. Supp. 2d 66, 83 (D.Conn. 2005) ("The court finds that it is appropriate to grant a brief stay of a preliminary injunction in order to permit the Court of Appeals an opportunity to consider an application for a stay pending an expedited appeal."); *Luevano v. Homer,* No. 79-0271, 1988 WL 147603, at *8 (D.D.C. June 27, 1988) ("[T]he Court will enter the injunctive relief that has been requested by plaintiffs but will, *sua sponte,* stay the effect of that injunction pending the outcome of the appeal in [a related case]. In this way, the interests of justice will best be served.").

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION, *et al.*,	:	13 Civ. 3994 (WHP)
Plaintiffs,	:	MEMORANDUM & ORDER
-against-	:	(Filed Dec. 27, 2013)
JAMES R. CLAPPER, *et al.*,	:	
Defendants.	:	

WILLIAM H. PAULEY III, District Judge:

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

Prior to the September 11th attacks, the National Security Agency ("NSA") intercepted seven calls made by hijacker Khalid al-Mihdhar, who was living in San Diego, California, to an al-Qaeda safe house in Yemen. The NSA intercepted those calls using overseas signals intelligence capabilities that could not capture al-Mihdhar's telephone number identifier. Without that identifier, NSA analysts concluded mistakenly that al-Mihdhar was overseas and not in the United

States. Telephony metadata would have furnished the missing information and might have permitted the NSA to notify the Federal Bureau of Investigation ("FBI") of the fact that al-Mihdhar was calling the Yemeni safe house from inside the United States.[1]

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

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

The natural tension between protecting the nation and preserving civil liberty is squarely presented by

---

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

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

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

BACKGROUND

I. Foreign Intelligence Surveillance Act

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

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

In 1978, Congress did just that. Legislating against the backdrop of *Keith* and the Church Committee findings, Congress enacted the Foreign Intelligence Surveillance Act of 1978 (FISA). Pub. L. No.

95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C: §§ 1801 to 1885c). FISA requires the Government to obtain warrants or court orders for certain foreign intelligence surveillance activities and created the FISC to review those applications and grant them if appropriate.

While the FISC is composed of Article III judges, it operates unlike any other Article III court. Proceedings in Article III courts are public. And the public enjoys a "general right to inspect and copy public records and documents, including judicial records and documents." *Nixon v. Warner Comm'cns, Inc.,* 435 U.S. 589, 597-98 (1978) (footnotes omitted). "The presumption of access is based on the need for federal courts, although independent – indeed, particularly because they are independent – to have a measure of accountability and for the public to have confidence in the administration of justice." *Lugosch v. Pyramid Co. of Onondaga,* 435 F.3d 110, 119 (2d Cir. 2006) (quoting *United States v. Amodeo,* 71 F.3d 1044, 1048 (2d Cir. 1995)); *see also Standard Chartered Bank Int'l (Americas) Ltd. v. Calvo,* 757 F. Supp. 2d 258, 259-60 (S.D.N.Y. 2010).[2]

[2] The Judicial Conference of the United States reaffirmed the public interest in the efficient and transparent administration of justice by acknowledging that "sealing an entire case file is a last resort." Judicial Conference of the United States, *Judicial Conference Policy on Sealed Cases* (Sept. 13, 2011), available at http://www.uscourts.gov/uscourts/News/2011/docs/JudicialConferencePolicyOnSealedCivilCases2011.p.

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

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

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

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

Bulk telephony metadata collection under FISA is subject to extensive oversight by all three branches of government. It is monitored by the Department of Justice, the intelligence Community, the FISC, and

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

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

> In accordance with the [FISA] Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The incidents, and the Court's responses, were also reported to the Intelligence Committees in great detail. The Committees, the Court, and the Executive Branch have responded actively to the incidents. The Court has imposed additional safeguards. In response to compliance

> problems, the Director of NSA also ordered 'end-to-end' reviews of the section 215 . . . programs, and created a new position, the Director of Compliance, to help ensure the integrity of future collection.

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

---

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

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

(Continued on following page)

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

In recognition of the broad intelligence gathering capability Congress granted to the Executive Branch, section 215 included a sunset provision terminating that authority at the end of 2005. But the war on terror did not end. Congress has renewed section 215 seven times.[4] In 2006, Congress amended section 215

> that the [FISC] will approve. That is hardly a rubber stamp. It's' rather extensive and serious judicial oversight of this process.

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

[4] *See* An Act to Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of that Act and the Lone Wolf Provision of the Intelligence Reform and Terrorism Provision Act of 2004 to July 1, 2006, Pub. L. No. 109-160, 119 Stat. 2957 (2005); An Act to Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of Such Act, Pub. L. No. 109-170, 120 Stat. 3 (2006); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006);

(Continued on following page)

to require the Government to provide "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106, 120 Stat. 192, 196 (2006) (codified as amended at 50 U.S.C. § 1861).

II. NSA Bulk Telephony Metadata Collection

On June 5, 2013, *The Guardian* published a then-classified FISC "Secondary Order" directing Verizon Business Network Services to provide the NSA "on an ongoing daily basis . . . all call detail records or 'telephony metadata'" for all telephone calls on its network from April 25, 2013 to July 19, 2013. *See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From Verizon Bus. Network Servs., Inc. ex. rel. MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.,* No. BR 13-80, slip op. at 2-4 (F.I.S.C. Apr. 25, 2013) ("*Secondary Order*"). "Telephony metadata" includes, as to each call, the telephone numbers that placed and received the call, the date, time, and duration of the call, other

---

Department of Defense Appropriations Act, 2010, Pub. L. No. 111-118, 123 Stat. 3409 (2009); An Act to Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, Pub. L. No. 111-141, 124 Stat. 37 (2010); FISA Sunsets Extension Act of 2011, Pub. L. No. 112-3, 125 Stat. 5 (2011); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011).

session-identifying information (for example, International Mobile Subscriber Identity number, International Mobile station Equipment Identity number, et cetera), trunk identifier, and any telephone calling card number. *See* Decl. of Teresa H. Shea, Director of the Signals Intelligence Directorate, NSA, dated Oct. 1, 2013, ¶ 15 (ECF No. 63); *Secondary Order* at 2. It does not include the content of any call, the name, address, or financial information of parties to the call, or any cell site location information. *See* Shea Decl. ¶ 15; *Secondary Order* at 2. In response to the unauthorized disclosure of the Secondary Order, the Government acknowledged that since May 2006, it has collected this information for substantially every telephone call in the United States, including calls between the United States and a foreign country and calls entirely within the United States. *See* Shea Decl. ¶ 13; White Paper at 3.

The Secondary Order was issued pursuant to a "Primary Order" setting out certain "minimization" requirements for the use of telephony metadata. *See In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From* [*REDACTED*], No. BPv 13-80 (F.I.S.C. Apr. 25, 2013) ("*Primary Order*"). The NSA stores the metadata in secure networks and access is limited to authorized personnel. *Primary Order* at 4-5. Though metadata for all telephone calls is collected, there are restrictions on how and when it may be accessed and reviewed. The NSA may access the metadata to further a terrorism investigation only by "querying" the database with a telephone

number, or "identifier," that is associated with a foreign terrorist organization. Shea Decl. ¶ 19; *Primary Order* at 6-9. Before the database may be queried, a high-ranking NSA official or one of twenty specially-authorized officials must determine there is "reasonable articulable suspicion" that the identifier is associated with an international terrorist organization that is the subject of an FBI investigation. Shea Decl. ¶¶ 20, 31; *Primary Order* at 7. The "reasonable articulable suspicion" requirement ensures an "ordered and controlled" query and prevents general data browsing. Shea Decl. ¶ 20. An identifier reasonably believed to be used by a U.S. person may not be regarded as associated with a terrorist organization solely on the basis of activities protected by the First Amendment. Shea Decl. ¶¶ 20, 31; *Primary Order* at 9. An identifier used to query telephony metadata is referred to as a "seed." Shea Decl. ¶ 20.

The results of a query include telephone numbers that have been in contact with the seed, as well as the dates, times, and durations of those calls, but not the identities of the individuals or organizations associated with responsive telephone numbers. Shea Decl. ¶ 21. The query results also include second and third-tier contacts of the seed, referred to as "hops." Shea Decl. ¶ 22. The first "hop" captures telephony metadata for the set of telephone numbers in direct contact with the seed. The second "hop" reaches telephony metadata for the set of telephone numbers in direct contact with any first "hop" telephone number. The third "hop" corrals telephony metadata for

the set of telephone numbers in direct contact with any second "hop" telephone number. Shea Decl. ¶ 22. The NSA takes this information and determines "which of the results are likely to contain foreign intelligence information, related to counterterrorism, that would be of investigative value to FBI (or other intelligence agencies)." Shea Decl. ¶ 26. They provide only this digest to the FBI. Moreover, metadata containing information concerning a U.S. person may only be shared outside the NSA if an official determines "that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance." *Primary Order* at 16-17; *see also* Shea Decl. ¶¶ 28, 32.

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

III. Plaintiffs' Claims

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

The Plaintiffs' employees routinely communicate by telephone with each other as well as with journalists, clients, legislators, and members of the public. The Plaintiffs' assert that "their" telephone records

"could readily be used to identify those who contact Plaintiffs . . . and is likely to have a chilling effect." Compl. ¶ 35. The Plaintiffs' seek a declaratory judgment that the NSA's metadata collection exceeds the authority granted by section 215 and violates the First and Fourth Amendments, and it also seeks a permanent injunction enjoining the Government from continuing the collection. Compl. ¶¶ 3638.

The Government moves to dismiss the complaint under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) for lack of standing and failure to state a claim. The ACLU moves under Rule 65 for a preliminary injunction barring the Government from "collecting [Plaintiffs'] call records" during the pendency of this action, requiring it to quarantine "all of [Plaintiffs'] call records [it] already collected," and enjoining the Government from querying metadata using any identifier associated with the Plaintiffs. Pls. Mot. For Prelim. Inj., dated Aug. 26, 2013 at 2 (ECF No. 26) [hereinafter "Pls. Mot."].

DISCUSSION

I. Standing

"[N]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies." *DaimlerChrysler Corp. v. Cuno,* 547 U.S. 332, 341 (2006) (internal quotation marks and alterations omitted); *see also Rothstein v. UBS AG,* 708 F.3d 82, 89-90 (2d Cir.

2013). The case-or-controversy requirement of Article III of the Constitution requires plaintiffs to establish their standing to sue. *Amnesty Int'l,* 133 S. Ct. at 1146 (citing *Raines v. Byrd,* 521 U.S. 811, 818 (1997)). "The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches." *Amnesty Int'l,* 133 S. Ct. at 1146. Therefore a court's standing inquiry is "especially rigorous" when the merits of the case would require the court "to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." *Amnesty Int'l,* 133 S. Ct. at 1147 (quoting *Raines,* 521 U.S. at 819-20).

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

telephone because they know the NSA will have a record that the call occurred.

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

[5] A panel in the Second Circuit adopted this novel view of standing. *See Amnesty Int'l USA v. Clapper.* 638 F.3d 118, 133-34, 139 (2d Cir. 2011), *overruled by* 133 S. Ct. 1138 (2013). This conclusion was criticized by other Second Circuit judges. *See Amnesty Int'l USA v. Clapper,* 667 F.3d 163, 194 (2d Cir. 2011) (denial of rehearing en banc) (Raggi, J. dissenting) (In finding that an "objectively reasonable likelihood" standard applied, "the panel did not explain its disregard of the Supreme Court's

(Continued on following page)

injury stemming from expensive precautions they took to avoid interception, such as traveling overseas to meet their clients in person instead of communicating electronically.

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

> (1) the Government will decide to target the communications of non-U.S. persons with whom [the plaintiffs] communicate;[6]

---

requirement that injury must be actual or imminently threatened"). The Supreme Court expressly rejected the Second Circuit's formulation. *See Amnesty Int'l* 133 S. Ct. at 1146, 1151.

[6] The *Amnesty International* plaintiffs were all U.S. persons. The FISA Amendments Act permits the NSA to intercept communications of U.S. persons only if they communicate with a non-U.S. person reasonably believed to be outside the United

(Continued on following page)

> (2) in doing so, the Government will choose to invoke its authority under [the FISA Amendments Act] rather than utilizing another method of surveillance,
>
> (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy [the FISA Amendments Act's] many safeguards and are consistent with the Fourth Amendment;
>
> (4) the Government will succeed in intercepting the communications of respondents' contacts; and
>
> (5) respondents will be parties to the particular communications that the Government intercepts.

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

The *Amnesty International* plaintiffs fared no better with their second alleged injury – costly precautions taken to avoid the risk of surveillance. In the

---

States who is the target of the surveillance. *See Amnesty Int'l,* 133 S. Ct. at 1144, 1148.

Supreme Court's view, that the plaintiffs "incurred certain costs as a reasonable reaction to a risk of harm" was insufficient "because the harm [plaintiffs sought] to avoid [was] not certainly impending." *Amnesty Int'l,* 133 S. Ct. at 1151. "Because respondents do not face a threat of certainly impending interception under [the FISA Amendments Act], the costs that they have incurred to avoid surveillance are simply the product of their fear of surveillance . . . such a fear is insufficient to create standing." *Amnesty Int'l,* 133 S. Ct. at 1152 (citing *Laird v. Tatum,* 408 U.S. 1, 10-15 (1972)).

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

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

Grp. v. S.W.I.F.T. SCRL, 607 F. Supp. 2d 500, 508 (S.D.N.Y. 2009)). But because Amidax could not plausibly show the Government had collected its records, it lacked standing. *Amidax,* 671 F.3d at 148-49.

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

The Government argues that merely acquiring an item does not implicate a privacy interest, but that is not an argument about Article III standing. Rather, it speaks to the merits of a Fourth Amendment claim. *Cf. Rakas v. Illinois,* 439 U.S. 128, 139 (1978) ("Rigorous application of the principle that the rights secured by the [Fourth] Amendment are personal, in place of a notion of "standing" will produce no additional situations in which evidence must be excluded. . . . [T]he better analysis . . . focuses on the extent of particular [individual's Fourth Amendment] rights, rather than on any theoretically separate, but

invariably intertwined concept of standing.") The ACLU is not obligated at the standing stage to prove the merits of its case, only that it has "a personal stake in this litigation." *Amidax,* 671 F.3d at 147. Because the ACLU has alleged an actual injury grounded in the Government's collection of metadata related to its telephone calls, it has standing.

II. Statutory Claim

A. Sovereign Immunity

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

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

F.3d 164, 171 (2d Cir. 2006) (quoting *Japan Whaling Ass'n v. Am. Cetacean Soc'y,* 478 U.S. 221, 230 n.4 (1986)). But the presumption favoring judicial review, "like all presumptions used in interpreting statutes, may be overcome by specific language or specific legislative history that is a reliable indicator of congressional intent." *Block v. Cmty. Nutrition Inst.,* 467 U.S. 340, 349 (1984). In particular, "the presumption favoring judicial review of administrative action may be overcome by inferences of intent drawn from the statutory scheme as a whole." *Block,* 467 U.S. at 349.

1. Section 702 Exception

Section 702 does not "confer[ ] authority to grant relief if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought." 5 U.S.C. § 702. This carve out ensures that a plaintiff cannot "exploit[ ] the APA's waiver to evade limitations on suit contained in other statutes" because "[t]he waiver does not apply 'if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought' by the plaintiff." *Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak,* 132 S. Ct. 2199, 2204-05 (2012). Thus, "'[w]hen Congress has dealt in particularity with a claim and [has] intended a specified remedy' . . . to be exclusive, that is the end of the matter; the APA does not undo the judgment." *Pottawatomi Indians,* 132 S. Ct. at 2205 (alterations in original) (quoting *Block v. North Dakota ex rel. Bd. of Univ. & Sch. Lands,* 461 U.S. 273, 286 n.22 (1983)).

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

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

This interpretation of section 215 is buttressed by FISA's overall statutory scheme: in contrast to other FISA surveillance statutes, section 215 does not authorize any action for misuse of the information obtained. *Compare* 50 U.S.C. § 1861 (use of information obtained from "tangible things" order not subject to redress under section 2712) with 50 U.S.C.

---

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

§ 1806(a) (use of information obtained from electronic surveillance actionable under section 2712); 50 U.S.C. § 1825(a) (same for physical searches); 50 U.S.C § 1845(a) (same for pen registers and trap and trace devices). Thus, Congress withdrew the APA's waiver of sovereign immunity for section 215. *See Pottawatomi Indians,* 132 S. Ct. at 2204-05; *see also Klayman,* 2013 WL 6571596, at *12 n.30; *Jewel* 2013 WL 3829405, at *12.

2. Section 701 Exception

Section 701 of the APA withdraws the immunity waiver "to the extent the relevant statute 'preclude[s] judicial review.'" *Block,* 467 U.S. at 345 (alterations in original) (citing 5 U.S.C. § 701(a)(1)). "Whether and to what extent a particular statute precludes judicial review is determined not only from its express language, but also from the structure of the statutory scheme, its objectives, its legislative history, and the nature of the administrative action involved." *Block,* 467 U.S. at 345.

In *Block,* the Supreme Court held that a milk consumer's challenge to milk market orders issued under the Agricultural Marketing Agreement Act was precluded under APA section 701(a)(1). 467 U.S. at 347. As the Supreme Court explained, the Agricultural Marketing Agreement Act "contemplates a cooperative venture" between the Secretary of Agriculture, milk handlers, and milk producers. *Block,* 467 U.S. at 346. For example, the Agricultural

Marketing Agreement Act provides for "agreements among the Secretary, producers, and handlers, for hearings among them, and for votes by producers and handlers." *Block,* 467 U.S. at 346-47 (internal citations omitted). The Agricultural Marketing Agreement Act requires a handler to exhaust administrative remedies before it permitted any judicial review. *Block,* 467 U.S. at 346. But the Agricultural Marketing Agreement Act was silent regarding milk consumers' remedies.

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

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

The "cooperative venture" envisioned by FISA's statutory scheme does not involve a mundane subject like milk pricing – it involves national security, a matter of vital importance. Congress's intent to keep the means and methods of the Government's intelligence gathering efforts secret from its enemies lies at the heart of FISA. Section 215 limits disclosure of orders to the narrowest group of individuals: (1) those to whom disclosure is necessary to comply with such

an order; (2) an attorney to obtain legal advice on how to respond to the order; and (3) other persons as permitted by the Director of the FBI. *See* 50 U.S.C. § 1861(d).[9] Section 215 does not just exclude a target from challenging an order, it precludes their participation in any way. *See Ark. Dairy Coop. Ass'n,* 573 F.3d at 822; *Block,* 467 U.S. at 346).

Allowing any challenge to a section 215 order by anyone other than a recipient would undermine the Government's vital interest in keeping the details of its telephone metadata collection program secret. It would also – because of the scope of the program – allow virtually any telephone subscriber to challenge a section 215 order. In *Koretoff v. Vilsack,* 614 F.3d 532, 537, (D.C. Cir. 2011) the D.C. Circuit discussed such an absurdity that also cropped up in *Block*. The D.C. Circuit noted that "[a]llowing suit by consumers would mean virtually every American could challenge every agricultural marketing

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

order. . . . [T]hat hard-to-fathom result was of great concern to the Supreme Court [in *Block*] and informed its assessment of Congress's intent on whether such suits were precluded by the [Agricultural Marketing Agreement Act]." *Koretoff,* 614 F.3d at 537. Allowing anyone but the recipient of section 215 orders to challenge them, or to do so anywhere outside the FISC, "would severely disrupt this complex and delicate administrative scheme." *Block,* 467 U.S. at 348. It is clear from the statutory scheme that Congress intended to preclude statutory causes of action such as this.

Of course, this says nothing about the ACLU's constitutional claims and it is hard to image a regime where they would be barred. A constitutional claim is precluded only on a "heightened showing" demonstrating a clear intent to do so. *Webster v. Doe,* 486 U.S. 592, 603 (1988). And there is no language in FISA expressly barring a constitutional claim. *See Klayman,* 2013 WL 6571596. at *13.

Regarding the statutory arguments, there is another level of absurdity in this case. The ACLU would never have learned about the section 215 order authorizing collection of telephony metadata related to its telephone numbers but for the unauthorized disclosures by Edward Snowden. Congress did not intend that targets of section 215 orders would ever learn of them. And the statutory scheme also makes clear that Congress intended to preclude suits by targets even if they discovered section 215 orders implicating them. It cannot possibly be that

lawbreaking conduct by a government contractor that reveals state secrets – including the means and methods of intelligence gathering – could frustrate Congress's intent. To hold otherwise would spawn mischief: recipients of orders would be subject to section 215's secrecy protocol confining challenges to the FISC, while targets could sue in any federal district court. A target's awareness of section 215 orders does not alter the Congressional calculus. The ACLU's statutory claim must therefore be dismissed.

B. Merits of the Statutory Claims

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

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

Section 215 was enacted at the same time as an amendment to the Stored Communications Act.

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

By contrast, section 215 allows the government an order "requiring the production of any tangible thing." Prior to its amendment, the Government's FISA authority to collect business records applied only to records from "common carrier[s], public accommodation. facilit[ies], physical storage facilit[ies], or vehicle facilit[ies]." 50 U.S.C. § 1862 (2001). Section 215 broadened the Government's authority to seek records from additional businesses. *See* 50 U.S.C § 1861 (as amended, 2008). The only limitation – relevant here – on the types of records that may be obtained with a section 215 order are that they be

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

obtainable with a grand jury subpoena. *See* 50 U.S.C. § 1861(c)(2)(D). Section 215 contains nothing suggesting that it is limited by the Stored Communications Act. Nevertheless, Plaintiffs argue that section 215 should be interpreted narrowly to avoid any conflict with the Stored Communications Act.

But this court must attempt to interpret a statute "as a symmetrical and coherent regulatory scheme, and fit, if possible, all parts into an harmonious whole" and is "guided to a degree by common sense." *Food & Drug Admin. v. Brown & Williamson Tobacco Corp.,* 529 U.S. 120, 133 (2000). Read in harmony, the Stored Communications Act does not limit the Government's ability to obtain information from communications providers under section 215 because section 215 orders are functionally equivalent to grand jury subpoenas. Section 215 authorizes the Government to seek records that may be obtained with a grand jury subpoena, such as telephony metadata under the Stored Communications Act.

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

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

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

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

"Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change." *Forest Grove Sch. Dist. v. T.A.,* 557 U.S. 230, 239-40 (2009) (quoting *Lorillard v. Pons,* 434 U.S. 575, 580 (1978)). "When 'all (or nearly all) of the' relevant judicial decisions have given a term or concept a consistent judicial gloss, we presume Congress intended the term or concept to have that meaning when it incorporated it into a later-enacted

statute." *Bruesewitz v. Wyeth LLC,* 131 S. Ct. 1068, 1082, 1082 (2011) (citing *Merck & Co. v. Reynolds,* 130 S. Ct. 1784, 1802 (2010)). "The consistent gloss represents the *public* understanding of the term." *Bruesewitz,* 131 S. Ct. at 1082.

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

The Congressional reports are not public and are submitted "in a manner consistent with the protection of the national security," namely, in classified, secret proceedings. 50 U.S.C. § 1871. Such

Congressional proceedings are akin to application process for a section 215 order and the FISC opinions on those applications – they are all classified, secret proceedings. There is no doubt that the Congressional Committees responsible for oversight of this program knew about the FISC opinions and the Executive Branch's interpretation of section 215. But what about the rest of Congress?

In 2010 and 2011, Congress reauthorized section 215 without making any changes.[11] Prior to the 2010 reauthorization, the Executive Branch made available *to all members of Congress* a classified, five-page document discussing the bulk telephony metadata program. On February 23, 2010, Senators Feinstein and Bond wrote to their colleagues:

> Members of the Select Committee on Intelligence have previously requested that the Executive Branch permit each Member of Congress access to information on the nature and significance of intelligence authority on which they are asked to vote. In response to these requests, the Attorney General and the Director of National Intelligence have provided a classified paper to the House and

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

> Senate Intelligence Committees on important intelligence collection made possible by authority that is subject to the approaching sunset, and asked for our assistance in making it available, in a secure setting, directly and personally to any interested Member.

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

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

The following year, when section 215 was again scheduled to sunset, senators were informed of an updated classified document available for their review. *See* Letter from Sens. Feinstein & Chambliss to Colleagues (Feb. 8, 2011) (ECF No. 33-11). Apparently

some Senators did review it,[12] while other Members of Congress did not.[13] The House Intelligence Committee did not make the document available to members of the House. Dozens of House members elected in 2010

---

[12] For example, Senator Wyden stated, "[M]any Members of Congress have no idea how the law is being secretly interpreted by the Executive Branch." and Senator Udall echoed that sentiment: "[W]hat most people – including many Members of Congress – believe the PATRIOT Act allows the government to do . . . and what government officials privately believe the PATRIOT Act allows them to do are two different things." *See* 157 Cong. Rec. S3386 (daily ed. May 26, 2011). At the time, Senators Wyden and Udall's remarks precipitated a Freedom of Information Act lawsuit by The New York Times seeking disclosure of the classified report to Congress. That case was assigned to this Court. After briefing, argument, and an *in camera* review, this Court concluded that disclosure of the report would "enable America's adversaries to develop means to degrade and evade the nation's foreign intelligence collection capabilities" and that it would "reveal and potentially compromise intelligence sources and methods." *N.Y. Times Co. v. U.S. Dep't of Justice,* 872 F. Supp. 2d 309, 316-17 (S.D.N.Y. 2012).

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

therefore never had an opportunity to review the classified document. While this is problematic, the Executive Branch did what it was required to do under the statutory scheme that Congress put in place to keep Congress informed about foreign intelligence surveillance.

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

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

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

A grand jury subpoena permits the Government to obtain tangible things unless "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation." *United States v. R. Enters., Inc.,* 498 U.S. 292, 301 (1991). The ACLU argues that the category at issue – all telephony metadata – is too broad and contains too much irrelevant information. That argument has no traction here. Because without all the data points, the Government cannot be certain it connected the pertinent ones. As FISC Judge Eagan noted, the collection of virtually all telephony metadata is "necessary" to permit the NSA, not the FBI, to do the algorithmic data analysis that allow the NSA to determine "connections between known and unknown international terrorist operatives." *In re Application of the Fed. Bureau of Investigation for*

an Order Requiring the Prod. of Tangible Things from [*REDACTED*], amended slip op. at 22-23. And it was the FISC that limited the NSA's production of telephony metadata to the FBI. While section 215 contemplates that tangible items will be produced to the FBI, FISC orders require that bulk telephony metadata be produced directly – and only – to the NSA. And the FISC forbids the NSA from disseminating any of that data until after the NSA has identified particular telephony metadata of suspected terrorists. Without those minimization procedures, FISC would not issue any section 215 orders for bulk telephony metadata collection. *In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from* [*REDACTED*], amended slip op. at 23.

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

Under section 215, the Government's burden is not substantial. The Government need only provide "a statement of facts showing that there are *reasonable grounds to believe* that the tangible things sought are relevant." 50 U.S.C. § 1861(b)(2)(A) (emphasis added). Because section 215 orders flow from the Government's grand jury and administrative subpoena powers, *see* 50 U.S.C. § 1861, the Government's applications are subject to deferential review. *See R. Enters., Inc.,* 498 U.S. at 301 (upholding grand jury subpoena challenged on relevancy grounds unless "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation"); *Nat'l Labor Relations Bd. v. Am. Med. Response, Inc.,* 438 F.3d 188, 193 (2d Cir. 2006) (finding that for an administrative subpoena, "the agency's appraisal of relevancy" to its investigation "must be accepted so long as it is not obviously wrong"). FISA applications for section 215 orders "are subject to 'minimal scrutiny by the courts;' both upon initial presentation and subsequent challenge." *United States v. Abu-Jihaad,* 630 F.3d 102, 130 (2d Cir. 2010) (quoting *United States v. Duggan,* 743 F.3d 59, 77 (2d Cir. 1984)).

The concept of relevance in the context of an investigation does not require the Government to parse out irrelevant documents at the start of its investigation. Rather, it allows that Government to get a category of materials if the category is relevant. The question of the permissible scope is generally

"variable in relation to the nature, purposes and scope of the inquiry." *Okla. Press Pub. Co. v. Walling,* 327 U.S. 186, 209 (1946). Defining the reasonableness of a subpoena based on the volume of information to be produced would require the Government to determine wrongdoing before issuing a subpoena – but that determination is the primary purpose for a subpoena. *See Okla. Press Pub. Co.,* 327 U.S. at 201 (noting that administrative subpoenas are authorized "to discover and procure evidence, not to prove a pending charge or complaint, but upon which to make one"). And in the context of a counterterrorism investigation, that after-the-attack determination would be too late.

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

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

301 (8th Cir. 1987) (authorizing collection of all wire transactions over $1,000 for a 14-month period at a particular Western Union office).

Any individual call record alone is unlikely to lead to matter that may pertain to a terrorism investigation. Approximately 300 seeds were queried in 2012 and only a "very small percentage of the total volume of metadata records" were responsive to those queries." Shea Decl. ¶ 24. But aggregated telephony metadata is relevant because it allows the querying technique to be comprehensive. And NSA's warehousing of that data allows a query to be instantaneous. This new ability to query aggregated telephony metadata significantly increases the NSA's capability to detect the faintest patterns left behind by individuals affiliated with foreign terrorist organizations. Shea Decl. ¶¶ 46, 48. Armed with all the metadata, NSA can draw connections it might otherwise never be able to find.[15]

The collection is broad, but the scope of counterterrorism investigations is unprecedented. National security investigations are fundamentally different from criminal investigations. They are prospective – focused on preventing attacks – as opposed to the

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

retrospective investigation of crimes. National security investigations span "long periods of time and multiple geographic regions." Decl. of Robert J. Holley, FBI Acting Assistant Director of the Counterterrorism Division, dated Oct. 1, 2013, ¶ 18 (ECF No. 62). Congress was clearly aware of the need for breadth and provided the Government with the tools to interdict terrorist threats.

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

documents will likely return irrelevant documents – but only that portion of a subpoena seeking an irrelevant category of documents should be quashed.

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

III. Constitutional Claims

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

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

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

A. Fourth Amendment

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

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

[16] Here are just a few matters in which an individual has no constitutionally protected expectation of privacy. *See, e.g., United States v. Miller,* 425 U.S. 435, 441-43 (1976) (bank records); *Couch v. United States,* 409 U.S. 322, 335-36 (1973)

(Continued on following page)

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

(records given to accountant); *Hoffa v. United States,* 385 U.S. 293, 302-03 (1966) (information revealed to a confidant); *On Lee v. United States,* 343 U.S. 747, 971 (1952) (information revealed to a false friend); *see also United States v.Todisco,* 667 F.2d 255, 258 (2d Cir. 1981) (telephone numbers collected by a pen register). And some more recent iterations. *See, e.g., United States v. Perrine,* 518 F.3d 1196, 1204-05 (10th Cir. 2008) (subscriber information provided to an internet service provider); *United States v. Lifshitz,* 369 F.3d 173, 190 (2d Cir. 2004) (information from a home computer that is transmitted over the Internet or by email); *see also United States v. Meregildo,* 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (information provided to Facebook "friend"). For an excellent discussion on the third party doctrine, *see generally,* Orin S. Kerr, The Case for the Third Party Doctrine, 107 Mich. L. Rev. 561 (2009).

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

The ACLU argues that analysis of bulk telephony metadata allows the creation of a rich mosaic: it can "reveal a person's religion, political associations, use of a telephone-sex hotline, contemplation of suicide, addiction to gambling or drugs, experience with rape, grappling with sexuality, or support for particular political causes." Decl. of Edward Felten, Professor of Computer Science and Public Affairs, Princeton University, ¶ 42 (ECF No. 27). But that is at least

three inflections from the Government's bulk telephony metadata collection. First, without additional legal justification – subject to rigorous minimization procedures – the NSA cannot even query the telephony metadata database. Second, when it makes a query, it only learns the telephony metadata of the telephone numbers within three "hops" of the "seed." Third, without resort to additional techniques, the Government does not know who any of the telephone numbers belong to. In other words, all the Government sees is that telephone number A called telephone number B. It does not know who subscribes to telephone numbers A or B. Further, the Government repudiates any notion that it conducts the type of data mining the ACLU warns about in its parade of horribles.[17]

---

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

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

Alexander Testimony at 66.

The ACLU also argues that "[t]here are a number of ways in which the Government could perform three-hop analysis without first building its own database of every American's call records." Supp. Decl. of Edward Felten, ¶ 6 (ECF No. 68-1). That has no traction. At bottom, it is little more than an assertion that less intrusive means to collect and analyze telephony metadata could be employed. But, the Supreme Court has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment." *City of Ontario, Cal. v. Ouon,* 130 S. Ct, 2619, 2632 (2010) (citing *Vanonia School Dist. 47J v. Acton,* 515 U.S. 646, 115 S. Ct. 2386, 2396 (1995)). That judicial-Monday-morning-quarterbacking "could raise insuperable barriers to the exercise of virtually all search-and-seizure powers" because judges engaging in after-the-fact evaluations of government conduct "can almost always imagine some alternative means by which the objectives might have been accomplished." *Quon,* 130 S. Ct. at 2632 (internal quotation marks and citations omitted).

The ACLU's pleading reveals a fundamental misapprehension about ownership of telephony metadata. In its motion for a preliminary injunction, the ACLU seeks to: (1) bar the Government from collecting "Plaintiffs' call records" under the bulk telephony metadata collection program; (2) quarantine "all of Plaintiffs' call records" already collected under the bulk telephony metadata collection program; and (3) prohibit the Government from querying metadata

obtained through the bulk telephony metadata collection program using any phone number or other identifier associated with Plaintiffs. Pls. Mot. at 2.

First, the business records created by Verizon are not "Plaintiffs' call records." Those records are created and maintained by the telecommunications provider, not the ACLU. Under the Constitution, that distinction is critical because when a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information. *See Smith,* 422 U.S. at 742. Second, the Government's subsequent querying of the telephony metadata does not implicate the Fourth Amendment – anymore than a law enforcement officer's query of the FBI's fingerprint or DNA databases to identify someone. *See Maryland v. King,* 133 S. Ct. 1958, 1963-64 (2013). In the context of DNA querying, any match is of the DNA profile – and like telephony metadata additional investigative steps are required to link that DNA profile to an individual.

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

prohibit the grand jury from engaging in a 'dragnet' operation.") (citation omitted).

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

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

U.S. at 744-45. Inferior courts are bound by that precedent.

Some ponder the ubiquity of cellular telephones and how subscribers' relationships with their telephones have evolved since *Smith.* While people may "have an entirely different relationship with telephones than they did thirty-four years ago," *Klayman,* 2013 WL 6571596, at *21, this Court observes that their relationship with their telecommunications providers has not changed and is just as frustrating. Telephones have far more versatility now than when *Smith* was decided, but this case only concerns their use as telephones. The fact that there are more calls placed does not undermine the Supreme Court's finding that a person has no subjective expectation of privacy in telephony metadata. *See Smith,* 442 U.S. at 745. ("The fortuity of whether or not the [tele]phone company in fact elects to make a quasi-permanent record of a particular number dialed does not . . . make any constitutional difference. Regardless of the [tele]phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record.") Importantly, "what metadata is has not changed over time," and "[a]s in *Smith,* the *types* of information at issue in this case are relatively limited: [tele]phone numbers dialed, date, time, and the like." *Klayman,* 2013 WL 6571596, at *21 (emphasis in original). Because *Smith* controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment.

B. First Amendment

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

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

Keith, 407 U.S. at 313-14 (internal quotation marks and citation omitted).

The ACLU alleges that "[t]he fact that the government is collecting this information is likely to have a chilling effect on people who would otherwise contact Plaintiffs." Compl. ¶ 35. Significant impairments of first amendment rights "must withstand exacting scrutiny." *United States v. Alvarez,* 132 S. Ct.

2537, 2548 (2012); *see also Nat'l Commodity & Barter Ass'n v. Archer,* 31 F.3d 1521, 1531 n.4 (10th Cir. 1994); *In re Grand Jury Proceedings,* 776 F.2d 1099, 1102-03 (2d Cir. 1985). The Government contends, however, that "surveillance consistent with Fourth Amendment protections . . . does not violate First Amendment rights, even though it may be directed at communicative or associative activities." *Gordon v. Warren Consol. Bd. of Educ.,* 706 F.2d 778, 781 n.3 (6th Cir. 1983).

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

First Amendment challenge to the "mail cover" practice). And this consideration is built in to any section 215 application. *See* 50 U.S.C. § 1861 (requiring that the investigation not be conducted "solely upon the basis of activities protected by the [F]irst [A]mendment").

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

Any alleged chilling effect here arises from the ACLU's speculative fear that the Government will review telephony metadata related to the ACLU's telephone calls. For telephony metadata to be "used to identify those who contact Plaintiffs for legal assistance or to report human-rights or civil-liberties violations," Compl. ¶ 35, it must actually be reviewed and the identities of the telephone subscribers

determined. Fear that telephony metadata relating to the ACLU will be queried or reviewed or further investigated "relies on a highly attenuated chain of possibilities." *Amnesty Int'l,* 133 S. Ct. at 1148. "[S]uch a fear is insufficient to create standing," *Amnesty Int'l,* 133 S. Ct. at 1152. Neither can it establish a violation of an individual's First Amendment rights.

IV. Remaining Preliminary Injunction Considerations

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

Here, the balance of the equities and the public interest tilt firmly in favor of the Government's position. "Everyone agrees that the Government's interest in combating terrorism is an urgent objective of the highest order." *Holder v. Humanitarian Law*

Project, 130 S. Ct. 2705, 2724 (2010); *see also Haig v. Agee,* 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.") (internal quotation marks omitted); *In re Directives* [*REDACTED*] *Pursuant to Section 105B of the Foreign Intelligence Surveillance Act.* 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) ("[T]he relevant government interest – the interest in national security – is of the highest order of magnitude.").

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

the telephony metadata collection program "could not be completely replicated by other means." Shea Decl. ¶ 63.

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

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

- In January 2009, while monitoring an extremist in Yemen with ties to al-Qaeda, the NSA discovered a connection with Khalid Oazzani in Kansas City. NSA immediately notified the FBI, which discovered a nascent plot to attack the New York Stock Exchange. Using a section 215 order, NSA queried telephony metadata to identify potential connections. Three defendants were convicted of terrorism offenses.

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

Holley Decl. ¶ 24-26; Testimony before the House Permanent Select Committee on Intelligence, dated June 18, 2013, FBI Deputy Director Sean Joyce, at 12-13 (ECF No. 33-13) [hereinafter "Joyce Testimony"].

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

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

Joyce Testimony at 52.

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

Fifteen different FISC judges have found the metadata collection program lawful a total of thirty-five times since May 2006. *See* Holley Decl. ¶¶ 6, 11; *In re Application of the FBI for an Order Requiring*

the Prod. of Tangible Things From [*REDACTED*], No. BR 13-158 (F.I.S.C. Oct. 11, 2013). The Government argues that "Plaintiffs are asking this Court to conclude that the FISC exceeded its authority when it authorized the NSA's bulk collection of telephony metadata, and that this Court (without the benefit of the classified applications and information available to the FISC) should substitute its judgment for the decisions that the FISC reached [35] times." Gov't Prelim. Inj. Opp. Br. at 16-17 (ECF No. 61) (internal citation omitted).

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

There is no question that judges operate best in an adversarial system. "The value of a judicial proceeding . . . is substantially diluted where the process is ex *parte,* because the Court does not have available the fundamental instrument for judicial judgment: an adversary proceeding in which both parties may participate." *Carroll v. President & Comm'rs of Princess Anne,* 393 U.S. 175, 183 (1968). At its inception, FISC judges were called on to review warrant applications, a familiar role and one well-suited for a judge

to protect the rights of an individual in his absence. The FISC's role has expanded greatly since its creation in 1978.

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

CONCLUSION

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

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

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

"Liberty and security can be reconciled; and in our system they are reconciled within the framework of the law." *Boumediene,* 553 U.S. at 798. The success of one helps protect the other. Like the 9/11 Commission

observed: The choice between liberty and security is a false one, as nothing is more apt to imperil civil liberties than the success of a terrorist attack on American soil. The 9/11 Commission Report, at 395. A court's solemn duty is "to reject as false, claims in the name of civil liberty which, if granted, would paralyze or impair authority to defend [the] existence of our society, and to reject as false, claims in the name of security which would undermine our freedoms and open the way to oppression. *American Comm'cns Ass'n, C.I.O. v. Douds,* 339 U.S. 382, 445 (1950) (Jackson, J., concurring in part and dissenting in part).

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

Dated: December 27, 2013
New York, New York

SO ORDERED:

/s/ William H. Pauley
WILLIAM H. PAULEY III
U.S.D.J.

Counsel of Record:
Jameel Jaffer, Esq.
Alex A. Abdo, Esq.
Brett M. Kaufman, Esq.
Patrick C. Toomey, Esq.
Catherine N. Crump, Esq.
American Civil Liberties Union
125 Broad Street
New York, NY 10004

Arthur N. Eisenberg, Esq.
Christopher T. Dunn, Esq.
New York Civil Liberties Union
125 Broad Street, 17th Floor
New York, NY 10004

Laura Donohue, Esq.
Georgetown Law
5417 Duvall Drive
Bethesda, MD 20816
Counsel for Plaintiffs

David S. Jones, Esq.
Tara M. La Morte, Esq.
Christopher B. Harwood, Esq.
John D. Clopper, Esq.
U.S. Attorney's Office, S.D.N.Y.
86 Chambers Street
New York, NY 10007
Counsel for Defendants

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
LEADING INTELLIGENCE INTEGRATION

Foreign Intelligence Surveillance Court Approves Government's Application to Renew Telephony Metadata Program

---

January 3, 2014

Foreign Intelligence Surveillance Court Approves Government's Application to Renew Telephony Metadata Program

On several prior occasions, the Director of National Intelligence has declassified information about the telephony metadata collection program under the "business records" provision of the Foreign Intelligence Surveillance Act, 50 U.S.C. Section 1861 (also referred to as "Section 215"), in order to provide the public a more thorough and balanced understanding of the program. Consistent with his prior declassification decisions and in light of the significant and continuing public interest in the telephony metadata collection program, DNI Clapper has decided to declassify and disclose publicly that the government filed an application with the Foreign Intelligence Surveillance Court seeking renewal of the authority to collect telephony metadata in bulk, and that the court renewed that authority on January 3, 2014.

It is the administration's view, consistent with the recent holdings of the United States District Courts for the Southern District of New York and Southern

District of California, as well as the findings of 15 judges of the Foreign Intelligence Surveillance Court on 36 separate occasions over the past seven years, that the telephony metadata collection program is lawful. The Department of Justice has filed an appeal of the lone contrary decision issued by the United States District Court for the District of Columbia.

Nevertheless, the Intelligence Community continues to be open to modifications to this program that would provide additional privacy and civil liberty protections while still maintaining its operational benefits. To that end, the Administration is carefully evaluating the recommendation of the President's Review Group on Intelligence and Communications Technologies regarding transitioning the program to one in which the data is held by telecommunications companies or a third party. In addition, the Privacy and Civil Liberties Oversight Board will complete a report on this program in the near future. The Administration will review all of these recommendations and consult with Congress and the Intelligence Community to determine if there are ways to achieve our counterterrorism mission in a manner that gives the American people greater confidence.

The Administration is undertaking a declassification review of this most recent court order.

Shawn Turner
Director of Public Affairs
Office of the Director of National Intelligence