

**KLAYMAN et al., Plaintiffs,**

**v.**

**OBAMA et al., Defendants.**

**Klayman et al., Plaintiff,**

**v.**

**Obama et al., Defendants.**

**Civil Action No. 13-0851 (RJL)**

United States District Court,  
District of Columbia.

Filed December 16, 2013

**Background:** Subscribers to certain telecommunications and Internet services brought actions against federal government and private service providers and their executive officers, challenging the constitutionality and statutory authorization of certain of government's intelligence-gathering practices relating to wholesale collection of phone record metadata for United States citizens and analysis of that data through National Security Administration (NSA). Subscribers moved for preliminary injunction to bar government from continuing to engage in bulk collection and querying of phone record metadata, and to require government to destroy any such metadata in its possession.

**Holdings:** The District Court, Richard J. Leon, J., held that:

- (1) court was barred from reviewing subscribers' claim that program exceeded government's statutory authority, in violation of Administrative Procedure Act (APA);
- (2) subscribers had standing to raise Fourth Amendment challenge to collection and querying components of program;
- (3) program constituted search under Fourth Amendment;
- (4) subscribers were likely to succeed in showing that government's searches

and NSA's analysis were unreasonable under Fourth Amendment;

- (5) subscribers demonstrated irreparable harm and public interest to support injunctive relief; and
- (6) order would be stayed pending appeal, in light of national security interests and novelty of constitutional issues.

Motions granted in part and denied in part, and order stayed 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.<sup>8</sup> 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 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.<sup>9</sup>

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

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/press-releases/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 Col-*

*lection 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>; 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/>.

Follow-on media reports 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.<sup>10</sup>

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 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 in-

vestigators, 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.<sup>11</sup> 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 its statutory authority under FISA.<sup>12</sup> 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*, — U.S. —, 133 S.Ct. 1138, 1143, 185 L.Ed.2d 264 (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

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

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

12. Plaintiffs also allege certain statutory violations by the private company defendants, Sec-

ond 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.

“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 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).<sup>13</sup>

In addition to authorizing wiretaps, §§ 1801–1812, FISA was subsequently amended to add provisions enabling the Government to obtain ex parte orders au-

thorizing 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 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 (includ-

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 Rehnquist’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 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.).

ing 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 nonpub-

licly 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).<sup>14</sup> The FISC review pool judge considering 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).

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.*

15. In addition to alleging that the NSA has “direct access” to Verizon’s databases, Sec-

## 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.<sup>15</sup> 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, compile, 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, 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 Or-

ond 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.

der, *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”).<sup>16</sup> 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.<sup>17</sup> Through targeted computerized searches of 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,<sup>18</sup> 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. 16; 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 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

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 history of the Bulk Telephony Metadata Pro-

gram, 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.

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.<sup>19</sup> An “identifier” (i.e., selection term, or search 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.<sup>20</sup> 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 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.<sup>21</sup>

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 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.

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



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.<sup>22</sup> According to the Government, following the “chains of communication”—which, for chains that cross different communications networks, is only possible 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

same seed identifier can be queried more than once over time, can generate 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, 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.

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 ev-

ery 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.<sup>23</sup> As a consequence, Judge 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

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 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.

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 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).<sup>24</sup> 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.<sup>25</sup>

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>.

[17, 18] 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 Govern-

ment obtains information by physically intruding on a constitutionally protected area,” *United States v. Jones*, — U.S. —, 132 S.Ct. 945, 950 n.3, 181 L.Ed.2d 911 (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, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring)). This case obviously does not involve a physical intrusion, and plaintiffs do not claim otherwise.<sup>41</sup>

[19] 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, 121 S.Ct. 2038 (whether a search has occurred is an “antecedent question” to whether a search was reasonable).<sup>42</sup>

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, 104 S.Ct. 1652, 80 L.Ed.2d 85 (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.

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*, 560 U.S. 746, 130 S.Ct.

#### 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, 99 S.Ct. 2577, 61 L.Ed.2d 220 (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, 99 S.Ct. 2577. 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 victim on one occasion.<sup>43</sup> *Id.* 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, 99 S.Ct. 2577. The main thrust of the Government’s argument here

2619, 2629, 177 L.Ed.2d 216 (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.

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).

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, 99 S.Ct. 2577—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—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*, — U.S. —, 132 S.Ct. 945, 181 L.Ed.2d 911 (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, 103 S.Ct. 1081, 75 L.Ed.2d 55 (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.”<sup>44</sup> *Id.* at 281, 103 S.Ct. 1081. 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 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*, — U.S. —, 132 S.Ct. 945, 181 L.Ed.2d 911 (“*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, 103 S.Ct. 1081)).<sup>45</sup>

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.

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, 106

[20, 21] 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 Telephony Metadata Program.<sup>46</sup> 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 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, 99 S.Ct. 2577. 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!

[22] 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, 99 S.Ct. 2577 ("[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

S.Ct. 1809, 90 L.Ed.2d 210 (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.").

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, 103 S.Ct. 1081); see also *id.* at 956, n.\* (Sotomayor, J., concurring). That the Court in *Smith* did not explic-

itly 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, 121 S.Ct. 2038 ("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?

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, 99 S.Ct. 2577, 61 L.Ed.2d 220; *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (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, 121 S.Ct. 1281, 149 L.Ed.2d 205 (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, 99 S.Ct. 2577, 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, 109 S.Ct. 1468, 103 L.Ed.2d 774 (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.”).<sup>47</sup>

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, 99 S.Ct. 2577. 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 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.*<sup>48</sup>

Finally, *and most importantly*, not only is the Government’s ability to collect,

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, 120 S.Ct. 1462, 146 L.Ed.2d 365 (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 manipu-

lation of petitioner’s bag violated the Fourth Amendment.”).

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”



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 modems.<sup>49</sup> CTIA—The Wireless Ass'n ("CTIA"), *Wireless Industry Survey Results—December 1985 to December 2012*, at 2, 6 (2013) ("CTIA Survey Results");<sup>50</sup> 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, IN-

DUS. ANALYSIS DIV., FED. COMM'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.<sup>51</sup> 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, 95-97% of adults age 18 to 49);<sup>52</sup> 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).<sup>53</sup> 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).<sup>54</sup> 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,

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).

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](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, *Wire-*

*less 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.

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>.

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.<sup>55</sup> Thirty-four years ago, city streets were lined with pay phones. Thirty-four years ago,

when people wanted to send “text messages,” they wrote letters and attached postage stamps.<sup>56</sup>

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.<sup>57</sup> But the ubiquity

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 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/resource-library/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, 99 S.Ct. 2577, 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*, 214 N.J. 564, 70 A.3d 630, 637–38 (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 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*

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, 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.<sup>58</sup> 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 (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.<sup>59</sup>

*States for an Order Directing a Provider of Elec. Comm'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 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.

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. Gov't'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.").

59. Public opinion polls bear this out. *See, e.g., Associated Press, 9/11 Anniversary: Poll finds public doubts growing on federal surveil-*

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.<sup>60</sup> The more difficult question, however, is whether their expectation of privacy is one that society is prepared to recognize as objectively reasonable and 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 reason-

able 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, 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.**

[23] 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, 126 S.Ct. 2193, 165 L.Ed.2d 250 (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*

*lance, 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, 99 S.Ct. 2577. 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 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*, 945 F.Supp.2d 769, 770–71, 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, 99 S.Ct. 2577. 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.*

*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, 117 S.Ct. 1295, 137 L.Ed.2d 513 (1997) (“To be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing.”).

[24–27] 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, 109 S.Ct. 1402, 103 L.Ed.2d 639 (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, 109 S.Ct. 1402). 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 individual-

ized suspicion in the particular context.’” *Id.* (quoting *Nat’l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665–66, 109 S.Ct. 1384, 103 L.Ed.2d 685 (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, 117 S.Ct. 1295, 137 L.Ed.2d 513)). 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, 122 S.Ct. 2559, 153 L.Ed.2d 735 (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, 122 S.Ct. 2559, 153 L.Ed.2d 735; *Vernonia Sch. Dist.*, 515 U.S. 646, 115 S.Ct. 2386, 132 L.Ed.2d 564; *Von Raab*, 489 U.S. 656, 109 S.Ct. 1384, 103 L.Ed.2d 685; *Skinner*, 489 U.S. 602, 109 S.Ct. 1402, 103 L.Ed.2d 639, and officers may search probationers and parolees to ensure compliance with the rules of supervision, see *Griffin v. Wisconsin*, 483 U.S. 868, 107 S.Ct. 3164, 97 L.Ed.2d 709 (1987).<sup>61</sup> The doctrine has also been applied in cases involving efforts to prevent acts of terrorism in crowded transportation centers. See, e.g., *Cassidy*

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, 107 S.Ct. 2636, 96 L.Ed.2d 601 (1987), searches of fire-damaged buildings for the purpose of determining the cause of the fire, see *Michigan v. Tyler*, 436

U.S. 499, 98 S.Ct. 1942, 56 L.Ed.2d 486 (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, 110 S.Ct. 2481, 110 L.Ed.2d 412 (1990); *United States v. Martinez-Fuerte*, 428 U.S. 543, 96 S.Ct. 3074, 49 L.Ed.2d 1116 (1976).

*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.

[28] 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 telephony metadata covering the last five years, and the NSA's Bulk Telephony Metadata Program significantly intrudes on that expectation.<sup>62</sup> 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, 122 S.Ct. 2559.

[29] The Government asserts that the Bulk Telephony Metadata Program serves the "programmable purpose" 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, 101 S.Ct. 2766, 69 L.Ed.2d 640 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation." (internal quotation marks omitted)).<sup>63</sup> A closer examination of the record, however, reveals that the Govern-

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.

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. Ressaam*, 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, 121 S.Ct. 447, 148 L.Ed.2d 333 (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.

ment'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 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 immi-

nent 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).<sup>64</sup> Given the limited record before me at this point in the 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

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

as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.<sup>65</sup> See *Chandler*, 520 U.S. at 318–19, 117 S.Ct. 1295 (“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 and therefore the NSA’s bulk collection program is indeed an unreasonable search under the Fourth Amendment.<sup>66</sup>

[30–32] 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, 99 S.Ct. 2577, *Miller*, 425 U.S. at 443, 96 S.Ct. 1619. 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 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, 121 S.Ct. 2038). 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, 87 S.Ct. 1727, 18 L.Ed.2d 930 (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,

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 & Theodor 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.”).

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, 121 S.Ct. 2038.



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, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (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.<sup>67</sup>

### **2. Plaintiffs Will Suffer Irreparable Harm Absent Injunctive Relief.**

[33, 34] “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, 96 S.Ct. 2673, 49 L.Ed.2d 547 (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 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.**

[35, 36] “[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*, — U.S. —, 134 S.Ct. 678, 187 L.Ed.2d 544, 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,

<sup>67</sup> 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.”).

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.<sup>68</sup> 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. . . .”).

69. For reasons stated at the outset, this relief is limited to *Klayman I* plaintiffs Larry Klay-

## 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<sup>69</sup> 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.<sup>70</sup>

[37] 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 ap-

man 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 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.

peal.<sup>71</sup> 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.