**IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA**

| | | |
|---|---|---|
| RAND PAUL, *et al.*, | ) | |
| | ) | |
| Plaintiffs | ) | |
| | ) | Civil Action No. |
| v. | ) | 1:14-cv-262-RJL |
| | ) | |
| BARACK OBAMA, *et al.*, | ) | |
| | ) | |
| Defendants. | ) | |

**PLAINTIFFS' OPPOSITION TO MOTION TO DISMISS**

Kenneth T. "Ken" Cuccinelli, II (*admitted pro hac vice*)
KCuccinelli@CuccinelliAndAssociates.com
Cuccinelli & Associates, PLLC
10560 Main Street, Ste. 218
Fairfax, Virginia 22030

Earl "Trey" Mayfield (D.C. Bar # 459998)
tmayfield@lewis-firm.com
Michael P. Lewis (D.C. Bar. # 503311)
mlewis@lewis-firm.com
The Lewis Firm, PLLC
901 New York Ave., Ste. 450E
Washington, D.C. 20001
Tel: 202-630-6006
Fax: 888-430-6695
*Counsel for Plaintiffs*

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES[†]

### Cases



[†] Pursuant to LCvR 7(a), authorities denoted with asterisks ** are those on which Plaintiffs chiefly rely.

**Statutes**



**FISC Opinions**



**Other Authorities**

**Regulations**

## INTRODUCTION

The Amended Complaint sets forth judicially cognizable violations of Plaintiffs' Fourth Amendment rights. The telephone metadata being seized and searched in this case is highly sensitive, personally revealing information about Plaintiffs' and Class Members' individual lives, including what they are doing, where they are located, and with whom they associate. Plaintiffs[1] have sought to protect that metadata by entering into contracts with their telephone service providers, contracts containing privacy provisions for the very purpose of excluding others, including the Government, from accessing such records. Not only do such contracts demonstrate Plaintiffs' reasonable privacy expectations in their metadata, but such contract rights alone suffice to bring the electronic records at issue within the Fourth Amendment's protections. This digital information is the modern-day equivalent of Fourth Amendment "papers."

The reasonableness of Plaintiffs' privacy expectations is reinforced by the numerous federal statutes implemented over the last three decades to protect the privacy of their telephone metadata. Society's widespread support for personal privacy expectations in telephone metadata is further demonstrated by state legislatures blocking their own law enforcement from using information generated from the challenged searches and seizures.

Finally, while Defendants contend *Smith v. Maryland*, 442 U.S. 735 (1979), controls here, the enormous differences between the single, reasonably articulated suspicion-based individual monitoring presented there and the suspicionless, society-wide ongoing seizure and searches under Government Defendants' Mass Associational Tracking Program ("MATP") are profound, rendering *Smith* inapposite. Accordingly, the Government's Motion to Dismiss should be denied.

## I. STANDARD OF REVIEW

On a motion to dismiss, the Court must accept as true all the factual allegations in the Complaint and construe all reasonable inferences therefrom in the light most favorable to Plaintiffs. *See Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555–56 (2007); *Atchinson v. Dist. of Co-*

[1] For instant purposes, the term "Plaintiffs" refers to both the named Plaintiffs and the putative class members.

*lumbia*, 73 F.3d 418, 422 (D.C. Cir. 1996). Through this lens, the Court must determine whether the well-pleaded factual allegations "plausibly give rise to an entitlement to relief." *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009). As the District of Columbia Circuit has emphasized, the plausibility standard does not impose a "probability requirement" at the pleading stage, but simply asks whether the Complaint presents sufficient facts to "permit a reasonable inference" that the Plaintiff has stated a claim. *Jones v. Horne*, 634 F.3d 588, 595 (D.C. Cir. 2011) (citing *Ashcroft*, 556 U.S. at 677). Moreover, a court may take judicial notice of public documents in a Rule 12(b)(6) motion without converting it to one for summary judgment. *Marshall Cty. Health Care Auth. v. Shalala*, 988 F.2d 1221, 1226, n.6 (D.C. Cir. 1993); *Fennell v. AARP*, 770 F. Supp. 2d 118, 124 n.3 (D.D.C. 2011).

## II. PLAINTIFFS HAVE STANDING TO SUE.

Plaintiffs have standing under Article III. They have suffered an injury because, as "subscriber[s] of both cellular and landline services," they "use[] and [have] used both cellular and/or landline telephones in the United States," from which "Defendants have, without legitimate legal basis, seized, stored, retained for five years, and periodically searched telephone metadata concerning every domestic or international telephone call" Plaintiffs have made since May 2006. (First Am. Compl. ("FAC") ¶¶ 4–5.) The injury is plainly traceable to the challenged conduct—the Government's collection of their call records. That injury is unquestionably redressable by the relief sought.

The Government argues Plaintiffs lack standing because (1) the Government asserts the MATP "has never captured information on all (or virtually all) telephone calls made and/or received in the United States"; (2) "the government has not declassified or otherwise acknowledged the identities of the carriers participating in the program," such that "it cannot be assumed" Plaintiffs' metadata has been produced to the NSA by their providers, AT&T and Verizon Wireless; and (3) the complaint "contains no allegations that the NSA has accessed or reviewed records of Plaintiffs' calls." (Gov't Br. 16, 17–18, 19.) These arguments are untenable.

Plaintiffs' challenge is not limited to the NSA's use of Plaintiffs' call records after collecting them but is also directed at the Government's collection of those records in the first place. *See, e.g.*, FAC ¶ 30 ("At a minimum, Defendants violate Plaintiffs' and class members Fourth Amendment rights each time they seize, store, or search Plaintiffs' and class members' telephone metadata."). The collection of Plaintiffs' call records is itself an injury sufficient for Article III; indeed, as the Complaint makes clear, the collection of Plaintiffs' call records constitutes a gross invasion of their privacy. *See, e.g.*, *ACLU v. Clapper*, 959 F. Supp. 2d 724, 738 (S.D.N.Y. 2013) ("[T]here is no dispute the Government collected telephony metadata related to the ACLU's telephone calls. Thus, the standing requirement is satisfied").

The Government's attempt to deny the standing injury created by its MATP collections reeks of duplicity. The Government is fully aware of the extent of its collection efforts and of the providers participating. Rather than simply admit Plaintiffs' data is targeted by the MATP and certainly seized via those efforts, the Government resorts to semantic evasions. *See, e.g.*, Gov't Br. at 16 ("[A]lthough the Government has acknowledged that the Section 215 telephony metadata program is broad in scope and involves the aggregation of an historical repository of data collected from more than one provider ….). "A party having control of information bearing upon a disputed issue may be given the burden of bringing it forward and suffering an adverse inference from failure to do so." *Ala. Power Co. v. Fed. Power Comm'n*, 511 F.2d 383, 391 n.14 (D.C. Cir. 1974). "The production of weak evidence when strong is available can lead only to the conclusion that the strong would have been adverse." *Interstate Circuit, Inc. v. United States*, 306 U.S. 208, 226 (1939). Having full possession of its exact efforts to seize what belongs to Plaintiffs, the Government cannot claim concealing the injury it inflicts entitles it to pretend the injury has not occurred.

The Government's duplicity comes in tandem with its hypocrisy. Despite presenting a FISC opinion to demonstrate this Court's ostensible error in *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2014), even that opinion holds telephone providers have vicarious standing to contest Section 215 collection orders *on behalf of their customers*. *In re Application of the FBI for an*

*Order Requiring the Production of Tangible Things*, Dkt. No. BR 14-01, at 7–10 (FISC Mar. 20, 2014) (Collyer, J.) (Gov't Br. Ex. 4).[2] Furthermore, notwithstanding the Government's artifice that "the First Amended Complaint contains no well-pleaded, non-conclusory allegation that either [AT&T or Verizon Wireless] is now or has ever been a participating provider in the program" (Gov't Br. at 17), the public record establishes that, in fact, both Verizon and AT&T *admit* they are participants. *See, e.g.*, Verizon Transparency Report of 2013 Data; AT&T Transparency Report of 2013 Data.[3] As stated in the Verizon Report, "The table below sets forth the number of national security demands we received in 2013. We note that while we now are able to provide more information about national security orders that directly relate to our customers, reporting on other matters, such as any orders we may have received related to the bulk collection of non-content information, remains prohibited." This admission of a restriction on disclosures would be unnecessary if Verizon were not subject to FISA orders. *See also* Knutson, R., "Verizon Says It Received More Than 1,000 National Security Letters in 2013," *Wall St. Journal*, Jan. 22, 2014 (emphasis supplied).[4]

Assuming, *arguendo*, one were inclined to indulge the Government's assertion that the MATP does not collect "all" or "virtually all" U.S. call data, the standing requirement has never

---

[2] The government's presentation of the March 20 FISC opinion is of a piece with its approach to both facts and law: It decides which selected facts and FISC opinions—or pieces thereof—it will disclose. Moreover, this Court should limit its reliance on the reasoning of those decisions, even though they come from what is nominally denominated a "court," because FISC proceedings are very different from normal judicial processes. FISC proceedings are conducted *ex parte* and, thus, the decisions do not enjoy the benefit of the adversary process, a hallmark of Article III's "case or controversy" requirement and a guarantor that a court has been presented with all the relevant facts and law. *Cf. Carroll v. President & Comm'rs of Princess Anne*, 393 U.S. 175, 183 (1968) ("The value of a judicial proceeding … is substantially diluted where the process is *ex parte*, because the Court does not have available the fundamental instrument for judicial judgment: an adversary proceeding in which both parties may participate."). Because FISC decisions result from proceedings lacking the safeguards of the adversary process, their reasoning deserves skepticism when presented to a court bound by Article III's "case or controversy" requirement, which demands an adversary proceeding.

[3] http://transparency.verizon.com/us-data/national-security (as of May 19, 2014); http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html (as of May 19, 2014).

[4] http://online.wsj.com/news/articles/SB10001424052702303947904579336763951250166 (as of May 8, 2014).

required precision in ascertaining injury. Injury-in-fact requires only that there "be some threatened or actual injury resulting from the putatively illegal action." *Virginia v. Am. Booksellers Ass'n*, 484 U.S. 383, 392 (1988) (internal quotation marks and citations omitted). Even if Plaintiffs cannot (by dint of the Government's secrecy) point to a particular call whose data has been seized, that is of no moment. They need only show the injury is probable. *NRDC v. EPA*, 464 F.3d 1, 6–7 (D.C. Cir. 2006) (finding plaintiffs have standing where they can demonstrate a "substantial probability" of injury based on risk posed by challenged governmental activity); *see also Cronin v. FAA*, 73 F.3d 1126, 1130 (D.C. Cir. 1996) ("[A]n individual who belongs to a specific class made subject to a challenged testing regulation has standing to attack the regulation without offering evidence that he or she is particularly likely to be tested."); *Comm. for GI Rights v. Callaway*, 518 F.2d 466, 471–72 (D.C. Cir. 1975) (finding Army drug prevention program with general applicability that raised potential of violating individual soldiers' Fourth Amendment rights posed sufficient threatened injury to create standing). Indeed, the federal courts have held plaintiffs have standing when their personal data has been taken without their permission, even if they cannot demonstrate any adverse use of that data. *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) (unencrypted personal data on stolen laptop); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) (hacker obtained personal data). Given the Government's MATP objective of aggregating phone call data nationwide in order to conduct searches, it is a virtual certainty some of Plaintiff's calls will be swept in that dragnet, and they thus have more than a substantial probability of incurring that injury.

Even if the relevant question were whether the NSA had reviewed Plaintiffs' records, the Complaint states the Government has done so. Every time the NSA queries the call-records database, it reviews everyone's records to determine whether they, their contacts, or their contacts' contacts are connected to a phone number the NSA deems suspicious. *See* FAC ¶¶ 16–17, 20–26; *accord Klayman*, 957 F. Supp. 2d at 27–29 (describing the Government's querying of the database via the "seed and hop" method). Government officials have stated that the NSA conducted

hundreds of these queries in 2012 alone. *See* HJC Hearing at 29:33–36:00 (testimony of John C. Inglis, NSA Deputy Director).[5]

The Government's reliance on *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), is misplaced. In *Amnesty*, the Supreme Court held the plaintiffs lacked standing to bring a constitutional challenge to the FISA Amendments Act of 2008. *See id*. at 1142–43. The Court reached that conclusion, however, not because the plaintiffs failed to demonstrate that their communications had been "retrieved" from government databases, Gov't Br. 12, but because the plaintiffs failed to demonstrate their communications had been *collected at all*. *Amnesty*, 133 S. Ct. at 1147–50. Indeed, the Government did not dispute the plaintiffs in *Amnesty* would have standing if they could show the Government had collected their communications. It is only now, confronted with plaintiffs who make this showing, that the Government argues mere collection is not enough.[6] As this Court has previously held, however, the Government has abandoned that argument by conceding it has created a database that is and must be comprehensive if search queries are to be effective. *Klayman*, 957 F. Supp. 2d at 27.

[5] The government's theory appears to be that it has not searched Plaintiffs' call records unless the NSA finds, after querying its database, that Plaintiffs are linked to a targeted phone number. This is a *non sequitur*. An individual whose luggage is inspected has been searched even if the inspection turns up no contraband. A person whose home is subjected to thermal-imaging has been searched even if the scan does not show the person is growing marijuana. *Cf. Kyllo v. United States*, 533 U.S. 27 (2001). Whether a search has occurred does not turn on whether the search produces information the government regards as useful or incriminating.

[6] The Government's record of material misrepresentations both to federal courts—including the Supreme Court in *Amnesty*—and to Congress is both notorious and dismaying. On May 13, 2014, Senators Ron Wyden (D-Or.) and Mark Udall (D-Colo.) wrote a letter to the Solicitor General of the United States complaining the Government had failed to correct its misrepresentation to the Supreme Court in the *Amnesty* case that under Section 702 of the Foreign Intelligence Surveillance Act interception of the contents of communications of U.S. persons was confined to cases involving surveillance targets. In fact, interceptions were also made when the communications of citizens were "about" targeted individuals. The Government's misrepresentation to the Supreme Court was relevant to the plaintiffs' contested standing under Article III to bring suit and was incorporated into the Court's opinion. (As of May 15, 2014, the letter is available at https://www.documentcloud.org/documents/1159181-051314-udall-wyden-response-to-doj-response.html.) *See also* FAC ¶¶ 37–38. In light of its pattern of dishonesty, the Government's declarations purportedly describing the methods and effectiveness of the surveillance program under Section 215 of the Patriot Act or otherwise should not be taken at face value nor accorded judicial deference.

To the extent the Government's argument is that the "mere" collection of Plaintiffs' call records does not inflict an injury, that argument goes to whether Plaintiffs have a reasonable expectation of privacy—that is, to the merits—not standing. As the Supreme Court has observed, the definition of Fourth Amendment rights "is more properly placed within the purview of substantive Fourth Amendment law than within that of standing." *Minnesota v. Carter*, 525 U.S. 83, 88 (1998); *accord Rakas v. Illinois*, 439 U.S. 128, 139 (1978). Courts frequently analyze Fourth Amendment challenges at the merits stage, rather than as a question of standing. *See, e.g.*, *United States v. Lawson*, 410 F.3d 735, 740 n.4 (D.C. Cir. 2005); *United States v. Dubose*, 2006 U.S. Dist. LEXIS 21035, at *20 n.3 (D.D.C. Apr. 19, 2006) ("This principle [judicial scrutiny for a legitimate expectation of privacy] is all-too-often collapsed into and confused with the 'standing' requirements of Article III. Despite the analytically subtle distinction between the two concepts, they remain distinct."); *accord Klayman*, 957 F. Supp. 2d at 29. In any event, there can be no dispute that the bulk collection of Plaintiffs' call records gives them the stake in this litigation that Article III requires. *Steagald v. United States*, 451 U.S 204, 211–16 (1981).

## III. PLAINTIFFS HAVE A REASONABLE EXPECTATION OF PRIVACY IN THEIR PERSONAL TELEPHONE METADATA.

The Fourth Amendment "requires a determination of whether the disputed search and seizure has infringed an interest of [Plaintiffs] which the Fourth Amendment was designed to protect." *Rakas*, 439 U.S. at 140. That analysis is a fact-intensive inquiry that asks "whether the facts of a particular case give rise to a legitimate expectation of privacy." *Id*. at 143 & n.12, 144. In this case, the facts demonstrate that Plaintiffs' privacy expectation in their telephone metadata the Government seized, stored, and searched for five years is eminently reasonable. "The constant element in assessing Fourth Amendment reasonableness … is the great significance given to widely shared social expectations." *Georgia v. Randolph*, 547 U.S. 103, 111 (2006).

The Fourth Amendment's guarantees of privacy and security grew out of America's colonial experience with general warrants, known as "writs of assistance," issued by King George III. Such writs allowed the King's agents to conduct searches and seizures with no basis other than

their own suspicions. General warrants were abhorred by Americans and "were denounced by James Otis as 'the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book ….' The historic occasion of that denunciation … said John Adams, … 'was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." *Stanford v. Texas*, 379 U.S. 476, 481–82 (1965) (citing *Boyd v. United States*, 116 U.S. 616, 625 (1886)).

"[Courts] must assur[e] preservation of that degree of privacy ***against government*** that existed when the Fourth Amendment was adopted." *United States v. Jones*, 132 S. Ct. 945, 950 (2012) (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)) (emphasis supplied, second alteration in *Jones*).

### A. The Supreme Court Has Long Recognized the Fourth Amendment as a Bulwark Against Governmental Privacy Invasions Resulting from Technological Advances.

Judicial concerns about the Government's ability to conduct electronic searches and seizures were raised even before the advent of computers. In *Goldman v. United States*, Justice Murphy wrote that "the search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment." 316 U.S. 129, 139 (1942) (Murphy, J., dissenting).

In *Whalen v. Roe*, the Supreme Court wrote, "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." 429 U.S. 589, 605 (1977).[7] Presaging the MATP, Justice Brennan observed,

[7] In a footnote following the quoted statement, the *Whalen* Court cited: Boyer, Computerized Medical Records and the Right to Privacy: The Emerging Federal Response, 25 BUFFALO L. REV. 37 (1975); Miller, Computers, Data Banks and Individual Privacy: An Overview, 4 COLUM. HUMAN RIGHTS L. REV. 1 (1972); Miller, A., *The Assault on Privacy* (1971); and, via a "see also" citation, *Utz v. Cullinane*, 520 F.2d 467, 478–82 (1975).

> What is more troubling about this scheme … is the central computer storage of the data thus collected. … [A]s the example of the Fourth Amendment shows, the Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and *I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology*."

*Id.* at 606–07 (Brennan, J., concurring) (emphasis added). Five years later, in *United States v. Knotts*, the Court expressly left open the judiciary's ability to scrutinize the eventual technological availability of "'twenty-four hour surveillance of any citizen … without judicial knowledge or supervision.' … *[I]f such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable*." 460 U.S. 276, 283–84 (1982) (citations omitted and emphasis added). Those concerns have been brought to fruition by the use of nearly unimaginably powerful computing technology. Defendants in this case began casting that dragnet over seven years ago to sweep up the telephone metadata from every phone call made to, from, or within the United States.

The federal courts have continued to express concerns about the implications of rapidly changing electronic technology for the Fourth Amendment. *See, e.g.*, *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 771 (1989) ("The substantial character of that [privacy] interest is affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten long before …."); *Kyllo*, 533 U.S. at 34 ("The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."); *United States v. Maynard*, 615 F.3d 544, 565 (D.C. Cir. 2010) ("For … practical reasons, and not by virtue of its sophistication or novelty, the advent of GPS technology has occasioned a heretofore unknown type of intrusion into an ordinarily and hitherto private enclave."), *aff'd sub nom. United States v. Jones*, 132 S. Ct. 945 (2012).

### B. Society Has Enshrined Personal Telephone Data as Private by Repeatedly Enacting Federal Statutes Prohibiting the Release of Such Data to the Government over the Past Thirty Years.

The reasonableness of Plaintiffs' expectation of privacy in their telephone metadata is buttressed by the numerous statutes restricting electronic communications carriers from voluntarily disclosing customers' records to the Government. At least four federal statutes now enforce the public's privacy expectations in telephone metadata, either by prohibiting disclosure of phone records to the Government except under legal process based on individualized suspicion of wrongdoing, or restricting disclosure to non-governmental entities. Such statutes also conclusively demonstrate that over the past three decades society has viewed Plaintiffs' expectations of privacy as reasonable.

#### 1. The Stored Wire and Electronic Communications and Transactional Records Access Act

Enacted in 1986, the Stored Wire and Electronic Communications and Transactional Records Access Act ("1986 Electronic Communications Privacy Act"), 18 U.S.C. §§ 2701–12, established, among other things, that electronic communications companies may not provide communication records to the Government without legal process or consent of the customer. 18 U.S.C. § 2702(a)(3) ("[S]hall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service … to any governmental entity"). As is the case with the Fourth Amendment, this restriction was against the Government, not others. Thus, 18 U.S.C. § 2703(c)(6) notes in the section entitled "Exceptions for Disclosure of Customer Records" that such transaction records (but not call or e-mail contents) may be disclosed "to any person other than a governmental entity."

#### 2. The Cable Television Consumer Protection and Competition Act of 1992

Section 20 of the Cable Television Consumer Protection and Competition Act of 1992 amended 47 U.S.C. § 551(a)(2) to ensure that already-existing statutory privacy protections for cable *television* customers were extended to *landline and cellular telephone* customers in cases in which cable operators started providing such telephone services.

### 3. The Telecommunications Act of 1996

The Telecommunications Act of 1996 ("1996 Act") provides statutory privacy protection for call records in the hands of telephone companies. The 1996 Act explicitly states that "[e]very telecommunications carrier has a duty to protect the confidentiality of *proprietary* information of, and relating to, … customers …." 47 U.S.C. § 222(a) (emphasis added).[8]

Under § 222 of the 1996 Act, a telephone company may not disclose or permit access to a customer's individually identifiable "customer *proprietary* network information" ("CPNI") without that customer's consent, except to provide service or to comply with the law. *Id.* § 222(c)(1) (emphasis added); *see also* 47 C.F.R. Part 64, Subpart U (CPNI regulations). Thus, § 222's primary intent is to restrict what telephone companies can do with their customers' phone records and associated private information in order to safeguard customers' privacy. *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1237 (10th Cir. 1999) ("Congress' primary purpose in enacting § 222 was concern for customer privacy."); *see also Nat'l Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996, 1001 (D.C. Cir. 2009) (expressing the view that the interest in protecting consumer privacy goes much farther than the Tenth Circuit suggested in *U.S. West*.).

The 1996 Act defines CPNI as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier …." 47 U.S.C. § 222(h)(1).

CPNI matches up nearly identically with the metadata being seized by Defendants in this case:

[8] Congress recognized in statute the *proprietary* nature of telephone metadata. Such explicit recognition is consistent with the common law notion of 'holding' intangible property that predates the advent of electronic data. One may have a possessory interest in intangible property as readily as tangible property.

| Telephone Metadata[9] | CPNI Equivalent[10] |
|---|---|
| International Mobile Subscriber Identity | Technical configuration; type of use |
| International Mobile Equipment Identity | Technical configuration; type of use |
| Trunk Identifiers | Location |
| Each phone's calling-card numbers | Type of use |
| Time/Date of each call | Amount of use; billing information |
| Terminating number dialed for each call | Destination; billing information |
| Originating number for each call | Technical configuration; type of use; billing information |
| Duration of each call | Amount of use; billing information |

**4. The Telephone Records and Privacy Protection Act of 2007**

The 2007 Telephone Records and Privacy Protection Act ("TRPPA"), 18 U.S.C. § 1039, generally makes it unlawful to buy, sell, transfer, or receive "confidential phone records information"[11] of a telecommunications carrier or a provider of voice over IP services ("VOIP") "without prior authorization from the customer to whom such confidential phone records information relates." 18 U.S.C. §§ 1039(b)(1), (c)(1).

Crucially, Congress found in TRPPA that: (a) "the information contained in call logs may include a wealth of personal data"; (b) "call logs may reveal the names of telephone users' doctors, public and private relationships, business associates, and more"; (c) "call logs are typically maintained for the exclusive use of phone companies, their authorized agents, and authorized consumers"; and (d) "the unauthorized disclosure of telephone records … assaults individual privacy …." *See* Pub. L. 109-476, § 2, Jan. 12, 2007, 120 Stat. 3568. Congress could hardly have been clearer about the fact that society views Plaintiffs' privacy expectations as reasonable when it comes to protecting their telephone metadata.

---

[9] *In re Application of the FBI for an Order Requiring the Production of Tangible Things* [etc.], Dkt. No. BR 13-80 (FISC Apr. 25, 2013).

[10] 47 U.S.C. § 222(h)(1).

[11] The definition of "confidential phone records information" in 18 U.S.C. § 1039 is virtually identical to the definition of CPNI, and similarly includes the phone records collected by Defendants. 18 U.S.C. § 1039(h)(1) ("information that—(A) relates to the quantity, technical configuration, type, destination, location, or amount of use of a service offered by a covered entity, subscribed to by any customer of that covered entity, and kept by or on behalf of that covered entity solely by virtue of the relationship between that covered entity and the customer; (B) is made available to a covered entity by a customer solely by virtue of the relationship between that covered entity and the customer; or (C) is contained in any bill, itemization, or account statement provided to a customer by or on behalf of a covered entity solely by virtue of the relationship between that covered entity and the customer.").

Notably, Congress's conclusion that call logs can reveal the names of doctors, relationships, business associates, etc., was made knowing that call logs contain phone numbers and other data, not names. **Defendants vehemently protest that the information they are seizing does not identify anyone individually**; however, Defendants' position requires an intentional denial of easily-available information. Congress obviously thought differently.

These statutory protections demonstrate that telephone users' transmission of their calling information to telephone companies, which is necessary for the limited purpose of making calls, does not undercut the reasonableness of their privacy expectations. *See, e.g.*, *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) ("The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."). Nothing in § 215 of the Patriot Act remotely suggests the protections of any of the foregoing federal statutes have been repealed as they relate to the Government's seizure of personal telephone records without particularized evidence.[12]

### C. The Metadata Collected by the MATP Is Highly Personalized and Sensitive, Particularly in the Aggregate.

Contrary to Defendants' assertions, the telephone metadata being seized and searched is highly sensitive information "that reflects a wealth of detail about [one's] familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring). Edward Felten, Professor of Computer Science and Public Affairs at Princeton, has stated that "[a]lthough this metadata might, on first impression, seem to be little more than 'information concerning the numbers dialed,' analysis of telephony metadata often reveals information that could traditionally only be obtained by examining the contents of communications. That is,

[12] A co-author of the relevant Patriot Act provision expressed shock at the scope of the dragnet effort undertaken under the guise of § 215: "I do not believe the released FISA order is consistent with the requirements of the Patriot Act. How could the phone records of so many innocent Americans be relevant to an authorized investigation as required by the Act?" Letter from Rep. F. James Sensenbrenner to U.S. Attorney General Eric H. Holder, Jr., at 2 (June 6, 2013) (attached hereto as Exhibit A). If Defendants' scope of MATP collections shocked a co-author of § 215, then Plaintiffs' privacy expectations in their own phone records are surely reasonable.

metadata is often a proxy for content." Declaration of E. Felten, ¶ 39, filed in *ACLU v. Clapper*, No. 13 Civ. 3994 (WHP) (S.D.N.Y. 2013) (Dkt. Entry 27) ("Felten Dec.").

Empirical analysis confirms that telephone metadata reveals personally sensitive information: "We found that phone metadata is unambiguously sensitive, even in a small population and over a short time window. We were able to infer medical conditions, firearm ownership, and more, using solely phone metadata." Mayer, J., & Mutchler, P., "MetaPhone: The Sensitivity of Telephone Metadata," Web Policy Blog (Mar. 12, 2014)[13] ("Stanford Study"). The foregoing conclusions were reached with a sample size of less than 600 people over a time period of only approximately three months. *Id.*[14]

The invasive and revealing power of the compilation, storage, and mining of hundreds of millions of Americans' metadata over the course of five years is obvious. As the Stanford Study concluded: "The dataset that we analyzed in this report spanned hundreds of users over several months. Phone records held by the NSA and telecoms span millions of Americans over multiple years. Reasonable minds can disagree about the policy and legal constraints that should be imposed on those databases. The science, however, is clear: phone metadata is highly sensitive." *Id.*

The more data the Government gathers on other people, the more the Government is able to discern about any individual from that person's data alone. Professor Felten notes:

> [T]he power of metadata analysis and its potential impact upon the privacy of individuals increases with the scale of the data collected and analyzed. It is only through access to massive datasets that researchers have been able to identify or infer new and previously private facts about the individuals whose calling records make up the telephone databases. Just as multiple calls by the same person reveal more than a single call, so too does a database containing calling data about millions of people reveal more information about the individuals contained within it than a database with calling data about just one person.

[13] As of April 30, 2014, available at: http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.

[14] This is the only such study located by undersigned counsel.

Felten Dec. ¶ 62; *see generally* Russell, S. & Norvig, P., "Artificial Intelligence: A Modern Approach," Pearson Educ. Ltd. (3d ed. 2009).[15]

Indeed, the President's Review Group on Intelligence and Communications Technologies recently came to the same conclusion about the collected MATP data: "… it is often argued that the collection of bulk telephony meta-data does not seriously threaten individual privacy, because it involves only transactional information rather than the content of the communications. Indeed, this is a central argument in defense of the existing program …. But … the record of every telephone call an individual makes or receives over the course of several years can reveal an enormous amount about that individual's private life …." President's Review Group Report (Dec. 12, 2013) at 116–17.[16]

### D. Plaintiffs' Use of Contracts to Protect the Privacy of Their Metadata Justifies Fourth Amendment Protection.

#### 1. Plaintiffs Individually Demonstrated Their Expectation of Privacy in Their Metadata by Affirmatively Protecting It in Their Telephone Service Contracts.

"In considering the reasonableness of asserted privacy expectations, … the Court has examined whether a person invoking the protection of the Fourth Amendment took normal precautions to maintain his privacy …." *Rakas*, 439 U.S. at 152 (Powell, J., concurring) (citations omitted). Here, Plaintiffs have not simply "assumed" the unique data over which they share dominion and control—and participate in the creation of—with their telephone service providers will remain private from others. Rather, they have entered into contracts explicitly intended to provide that protection.

The challenges to Fourth Amendment analysis presented by digital information and computing can be addressed without a change in jurisprudence by analyzing contractual protections of digital information in the same manner as property protections in other contexts. Digital in-

[15] These kinds of analyses are also evidence for standing purposes of the injury plaintiffs have incurred. *Meese v. Keene*, 481 U.S. 465, 473–74 (1987).

[16] Available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (as of May 6, 2014).

formation is a 21st-century "paper" in Fourth Amendment parlance. *See, e.g.*, *United States v. Christie*, 717 F.3d 1156, 1166 (10th Cir. 2013) ("In an age where computers permit access to most every 'paper and effect' a person owns …."); *United States v. Wurie*, 728 F.3d 1 (1st Cir. 2013) (noting as part of holding that many Americans now store their "papers" and "effects" as electronic media on their cell phones), *cert. granted*, 134 S. Ct. 999 (2014). Such treatment is particularly appropriate where, as here, the Government is effectuating a modern equivalent of a "general warrant" from the colonial era—one of the Founders' primary inspirations for establishing Fourth Amendment protections in the first place.[17]

Treating contractual protections with the dignity of property rights is supported by the majority opinion in *Katz*.[18] "[W]hat a person ***knowingly exposes to the public***, even in his own home or office, is not a subject of Fourth Amendment protection. But what he ***seeks to preserve as private***, even in an area accessible to the public, may be constitutionally protected." *Katz*, 389 U.S. at 351–52 (emphasis added). Because Plaintiffs have excluded others from access to their telephone metadata by contract, they clearly have a possessory interest in their metadata that is interfered with when Defendants seize that metadata, even if such metadata is obtained from Plaintiffs' telephone service providers. *But see Klayman*, 957 F. Supp. 2d at 30 n.41 (no possessory interest identified).

The use of digital information involving more than a single person, such as telephone metadata, cloud storage, joint ownership, and simultaneous use, routinely requires affirmative

[17] *See* Dripps, D., *Dearest Property: Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49 (2013) (explaining how the seizure of papers to be later searched for evidence of criminality was considered to be a distinct abuse considered equally disturbing to that of using general warrants to search houses).

[18] Justice Harlan's famous formulation of the "reasonable expectation of privacy" test in his *Katz* concurrence is more frequently referenced in Fourth Amendment discussions, but as Justice Alito observed in *Jones*, that test "involves a degree of circularity, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks." *Jones*, 132 S. Ct. at 962 (Alito, J., concurring in judgment) (citations omitted). In addition, "the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations." *Id.*

steps to exclude the outside world—the "public"—from accessing that information.[19] Such steps greatly simplify the Fourth Amendment analysis under *Katz*, whether they be contract terms with a telephone service provider, password-protecting e-mail, or using "do not track" settings on an Internet browser. Courts need not speculate whether a subjective expectation of privacy exists where someone has taken active steps to deny the world at large access to the digital information at issue. Particularly in the electronic age, contract rights should be treated co-extensively with property rights in maintaining privacy protections; with digital information being intangible property, contract and property protections under the Fourth Amendment should be the same:

> Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society. One of the main rights attaching to property is the right to exclude others, *see* W. Blackstone, Commentaries, Book 2, ch. 1, and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by this right to exclude.

*Rakas*, 439 U.S. at 163 n.12.

Given that telephone communication has become a necessity of modern commercial life and ubiquitous in most Americans' private lives, even reflecting the phone owner's personal traits, it must be expected that personal data sufficient to carry on the subscriber–telephone company relationship will necessarily be maintained and/or generated by the telephone company. This is why well over half of all Americans' telephone service contracts include privacy protection provisions.[20]

In sum,

> it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *This approach is ill suited to the digital*

[19] Courts often treat the "public" as everyone else in the world, rather than only those outside of a defined circle of intended exposure, requiring secrecy as a prerequisite for privacy. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring). *Katz*'s majority rationale is more applicable in the digital age.

[20] For the cataloging of wireless subscribers in the United States, *see* http://en.wikipedia.org/wiki/List_of_United_States_wireless_communications_service_providers; for privacy terms for AT&T and Verizon subscribers (the two largest, totaling over 200 million), *see* http://www.att.com/gen/privacy-policy?pid=2506 (available as of Apr. 16, 2014) and http://www.verizon.com/about/privacy/policy/#insideVz (available as of Apr. 16, 2014).

> *age, in which people reveal a great deal of information about themselves to third parties* in the course of carrying out mundane tasks. … I would not assume that all information voluntarily disclosed to some member of the public *for a limited purpose* is, for that reason alone, disentitled to Fourth Amendment protection.

*Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (emphasis added; citation omitted); *see also* President's Review Group on Intelligence and Communications Technologies Report at 111–12. Society plainly views Plaintiffs' expectations of privacy regarding their telephone metadata as reasonable.

**2. Plaintiffs' Affirmative Measures to Protect Their Metadata by Contract Fall Well Within the Supreme Court's Traditional Standards for Protecting Private Information.**

The most important evidence of Plaintiffs' subjective privacy expectation in their telephone metadata is that they took the objectively observable affirmative step of entering into contracts with their telephone service providers to secure that privacy against all others outside their contractual relationship. Such affirmative steps constitute the type of evidence the majority in *Katz*, 389 U.S. at 351–52, identified for determining one's subjective expectation of privacy.

In *Rakas v. Illinois*, 439 U.S. 128 (1978), defendants were passengers in someone else's car and sought to suppress the results of a search of the car that turned up a rifle under the passenger seat and ammunition in the glove compartment. The defendants did not claim ownership of either the rifle or the ammunition. The Supreme Court rejected the defendants' Fourth Amendment claims, noting the defendants in that case "made no showing that they had any legitimate expectation of privacy in the glove compartment or area under the seat of the car in which they were merely passengers. … [T]hese are areas in which a passenger *qua* passenger simply would not normally have a legitimate expectation of privacy." *Id.* at 148–49. Comparing the *Rakas* defendants' situation to this case, telephone subscribers *qua* telephone subscribers *do* have a legitimate expectation of privacy in *their* telephone metadata when it is protected by explicit contract terms, as well as when such subscribers know (or believe they know) their metadata is also protected by statute. The *Rakas* defendants, by contrast, had no demonstrable basis for expecting privacy in someone else's car.

The *Rakas* Court's discussion of two other precedents is instructive here. *See Jones v. United States*, 362 U.S. 257 (1960) (hereafter "*1960 Jones*") (Fourth Amendment protects friend of apartment owner where such friend has been granted control of apartment);[21] *Katz*, 389 U.S. 347 (Fourth Amendment protects contents of telephone conversation made within phone booth).[22]

The *Rakas* Court first considered *1960 Jones*: "Jones not only [1] had permission to use the apartment [2] of his friend [3], but also had a key to the apartment [4] with which he admitted himself on the day of the search and kept possessions in the apartment. [5] Except with respect to his friend, Jones had complete dominion and control over the apartment and could exclude others from it." *Rakas*, 439 U.S. at 149. A similar comparison of the present case to *1960 Jones* leads to the following conclusions:

1. Analogous to Jones's permission to use the apartment, Plaintiffs have contractual permission to use the telephone system.

2. Plaintiffs' telephone service providers are analogous to Jones's friend.

3. Plaintiffs established technical access to the telephone system at the outset of the subscriber–telephone company relationship by mutual consent with the telephone service provider. Having such technical access is the equivalent of Jones's having a key to the apartment.

4. Plaintiffs admit themselves to the telephone system based upon their technical access, or "key," and they keep data with the telephone company, some intentionally placed with the telephone company (e.g., name and address) and some generically understood to be generated by the making and receiving of telephone calls (e.g., phone numbers dialed)—such data being analogous to Jones's possessions in the apartment.[23]

---

[21] *See also Minnesota v. Olson*, 495 U.S. 91 (1990) (finding overnight guest in duplex had reasonable expectation of privacy even though it was not his own home).

[22] For ease of comparison to the present case, bracketed, numbered notes have been added to the Court's language.

[23] A necessary element of Plaintiffs' relationships with their telephone service providers is that at least a copy of the data referenced herein must remain with the telephone company. Otherwise, Plaintiffs' phones could not connect to and utilize the phone system.

5. Based on the contract between each subscriber and telephone company, subscribers have dominion and control over their metadata and can exclude others from it aside from their telephone company itself.

The foregoing comparisons lead to the same conclusion as in *1960 Jones*—Plaintiffs' telephone metadata is protected by the Fourth Amendment, even in the possession of the telephone company; just as Jones was protected even in his friend's apartment.

The *Rakas* Court further noted, "Likewise in *Katz*, the defendant occupied the telephone booth, shut the door behind him to exclude all others and paid the toll, which 'entitled [him] to assume that the words he utter[ed] into the mouthpiece [would] not be broadcast to the world.'" *Rakas*, 439 U.S. at 149 (quoting *Katz*, 389 U.S. at 352) (alterations in *Rakas*). Similarly, here, other than necessarily exchanging information with their telephone service providers for the limited purpose of conducting calls and billing, Plaintiffs sought to exclude all others from access to their telephone metadata by entering into contracts with their telephone service companies, and paid their telephone bills as part of their contracts. As a result, Plaintiffs reasonably expected their sensitive metadata would neither be broadcast to the world nor handed over to the Government.

"Katz and Jones could legitimately expect privacy in the areas which were the subject of the search and seizure each sought to contest." *Rakas*, 439 U.S. at 149. So too here. Plaintiffs legitimately expect the maintenance of the privacy of their telephone metadata under the Fourth Amendment. "[T]he Fourth Amendment protects people, not places." *Katz*, 389 U.S at 351. Plaintiffs' contracts to preserve the privacy of their telephone metadata constitute objectively observable evidence of Plaintiffs' subjective expectation of privacy. "What a person ***knowingly exposes to the public***, even in his own home or office, is not a subject of Fourth Amendment protection. But what he ***seeks to preserve as private***, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351–52 (emphasis added and citations omitted).

### E. State Efforts Blocking Use of MATP Metadata and Other Electronically Gathered Evidence Further Demonstrate That Society Regards Expectations of Privacy in Telephone Metadata as Reasonable.

In 2013, after the MATP was publicly disclosed, public opinion polls showed widespread opposition to Defendants' dragnet seizure, storage, retention, and searching of telephone metadata.[24] Such polling results are one form of evidence showing society views Plaintiffs' subjective expectations as reasonable: namely, that telephone metadata related to their telephone calls will remain off-limits to Government seizure, storage, retention, and search absent particularized suspicion that such metadata is relevant to a specific law enforcement investigation. State legislatures have begun to reflect these sentiments.

As 2014 began, state legislatures began new sessions all over the country, and an extraordinary number of states advanced legislation responding to Defendants' MATP. These legislative efforts represent further evidence that society deems Plaintiffs' privacy expectations in telephone metadata as reasonable. The Government haughtily dismisses the states' actions as "irrelevant." (Gov't Br. at 30 n.16.) The Government is wrong. Legislative actions constitute highly convincing evidence of what American society as a whole considers reasonable. *See Bissonette v. Haig*, 800 F.2d 812, 814 (8th Cir. 1986) (en banc) ("Acts of Congress, which after all must be at least prima facie evidence of what society as a whole regards as reasonable, are among" the sources outside the Fourth Amendment from which legitimate expectations of privacy arise);[25] *id.* at 815 ("*Not only federal law, but also state law, can be relevant in determining what is reasonable* under the Fourth Amendment.").[26]

---

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

[25] Immediately prior to this statement, the Court quoted *Rakas*, 439 U.S. at 144, for the point that "[l]egitimation of expectations of privacy must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Bissonette*, 800 F.2d at 814.

[26] Similarly, data about standard practices in society or in particular industries may be informative. *See, e.g., United States v. Ziegler*, 456 F.3d 1138, 1144–46 (9th Cir. 2006) (noting relevance of trade association data showing percentage of employers monitoring employees' computer and phone usage when assessing employee's reasonable expectation of privacy in workplace computer or phone).

In the most direct examples of legislation specifically targeting the use of information generated without a warrant, including Defendants' MATP, thirteen states have bills at every stage, from mere submission through enactment, blocking their own law enforcement from using the fruits of the MATP. At present, such information can, in some instances, be shared with state fusion centers and in other ways be made available by the federal government to state and local law enforcement. The states working to block the use of MATP information by their own state's law enforcement include: Alaska, Arizona, California, Kansas, Maine, Michigan, Minnesota, Missouri, New Hampshire, Oklahoma, South Carolina, Utah, and Vermont.[27]

Moreover, fifteen states have enacted or are advancing legislation that forecloses their state and local governments from obtaining cell phone tracking information in the absence of particularized legal process, e.g., a warrant. These states include: Illinois, Maine, Michigan, Minnesota, Missouri, Montana, New Hampshire, Pennsylvania, Rhode Island, South Carolina, Tennessee, Utah, Virginia, West Virginia, and Wisconsin.[28]

Taken together, twenty-one different states representing nearly half of the U.S. population[29] have responded to the public disclosure of Defendants' seizing, storing, retaining, and searching of so many Americans' telephone metadata in ways broadly demonstrating that society views Plaintiffs' expectations of privacy in their telephone metadata as reasonable.

### F. *Smith v. Maryland* Is Inapplicable to This Case.

#### 1. The Circumstances Here Are Utterly Distinct from *Smith*'s.

Defendants overwhelmingly rely on *Smith v. Maryland*, 442 U.S. 735 (1979), in their arguments to dismiss Plaintiffs' case. That reliance is misplaced. The differences between the present case and *Smith* in circumstances, nature, and scope are so stark as to make *Smith* inapposite.

The pen register police placed on Smith's phone line at the phone company's central office revealed a phone call Smith made to the robbery victim on the very first day it was installed.

---

[27] As of May 19, 2014, information on the referenced legislative efforts in all of the cited states is available at: http://www.offnow.org/action/state.

[28] *Id.*

[29] *See* http://www.census.gov/popest/data/state/totals/2013/.

On that basis and on the basis of other evidence, Smith's residence was searched pursuant to a warrant. The search revealed other incriminating evidence and Smith was included in a lineup in which the robbery victim identified him as the robber, at which point he was arrested. *Id.* at 737.

In denying Smith's request to suppress the pen register evidence, the Supreme Court held no Fourth Amendment search had taken place and Smith had no reasonable expectation of privacy because he voluntarily shared his telephone information, in this case the phone number he dialed, with a third party—the phone company. *Id.* at 743 ("Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, *under these circumstances*, harbor any general expectation that the numbers they dial will remain secret.") (emphasis added). The Court went on to declare "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743–44.

In comparing "these circumstances" in *Smith* to the case at bar, the differences are many and significant. Such differences include the following:

a. In *Smith*, the car owned by the target of the information-gathering had previously been spotted in the crime victim's neighborhood three times, whereas in this case there is no indication beforehand that *any* information gathered is related to anyone who has anything to do with any crime whatsoever.

b. The crime perpetrator in *Smith* was known to have used a phone to call the victim, whereas in this case there is no known or suspected crime at the time of data collection.

c. The pen register in *Smith* was operational only for two days, whereas here the Government is in a permanent cycle of ongoing collection. Thus, the volume of data is exponentially greater than in *Smith*. What the Government can learn about any given individual from such comprehensive data gathering was beyond imagining at the time of *Smith*.

d. There was no expectation the data gathered in *Smith* would be kept after the robbery case was over, whereas in this case data is being seized, stored, kept, and searched for five years with no relation of Plaintiffs' data to any case whatsoever.

e. In *Smith*, the data gathered could have shown nothing about the movements of the caller, whereas the gathering of trunk identifying information under FISC orders for mobile phones provides approximate personal location over a long period of time. This reveals private information about Plaintiffs' travel, locations, and associations, even when such locations would be otherwise unobservable to law enforcement.

f. The relationship between the Government and the phone company in *Smith* was significantly different, i.e., limited in scope and cooperation, whereas the daily and systematic exchange of all telephone metadata in this case spanning over seven-and-a-half years puts the telephone companies in a different posture than was the case in *Smith*. *See US DoJ*, 489 U.S. at 764 (recognizing how a right to privacy may continue when "hard-to-obtain information" is compiled into a more readily-accessible form).

g. The Government's ability at the time of *Smith* to address many more than one or a few phone numbers in any coordinated fashion simply did not exist. By contrast, the Government's technical capability today to seize, store, and search *every single phone number in the entire country* was inconceivable to the Court in 1979, much less to the authors of the Fourth Amendment. This concern for the impact of technological advances that allow dramatically expanded reach of surveillance beyond the range of human senses, so disconnected from anything imaginable at the time of ratification of the Fourth Amendment, has been rising since the 1970s.

h. In *Smith*, nothing but the date, time, and phone numbers involved in a phone call were captured, whereas with the MATP, phone numbers, approximate location (via trunk identifier), whether or not a call was completed/connected, the date, time, and duration of call, and a variety of details about the specific phones used on both ends of each phone call are obtained by the Government. *See, e.g.*, *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); *Klayman*, 957 F. Supp. 2d at 15 & n.16 (citing said FISC order, which the Government filed as an exhibit in *Klayman* at Docket Entry 25-3).

i. In *Smith*'s time, there were only landlines. There was no notion of a "mobile" phone, as there were no cellular phone systems in the U.S. until the 1980s; whereas today the vast majority of American adults have a personal cell phone, and personal cellular telephone communication has reached such a level of ubiquity that our phone usage says much about us as individuals—something not even contemplated in 1979. Roughly the same proportion of adults had cell phones in 2013 (approx. 91%)[30] as households had landlines in 1979 (approx. 91%).[31]

j. At the time of *Smith*, Americans had no choices among phone companies. There was only AT&T. With that lack of choice among telephone service providers, there existed a concomitant lack of competition in the terms offered to subscribers. Thus, while Plaintiffs today are protected by *contractual privacy* terms, that was not the case for Mr. Smith. *See, e.g.*, privacy terms of Verizon Wireless contract at: http://www.verizon.com/about/privacy/policy/#insideVz (available as of Apr. 10, 2014). Similarly, Defendant Smith did not benefit from the *statutory* privacy protections implemented after *Smith* was decided.[32]

Given the vast differences in the circumstances between *Smith* and this case, the Court should find *Smith* inapplicable and deny Defendants' Motion to Dismiss.

**2. The "Third-Party Disclosure Doctrine" Does Not Apply Here.**

The Government's brief devotes ample attention to the notion that the so-called "third-party disclosure doctrine" purportedly derived from *Smith v. Maryland* and *United States v. Mil-*

[30] Brenner, J., Pew Internet: Mobile (Sept. 18, 2013), as of May 1, 2014, available at http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx.

[31] 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).

[32] In recent years the practice of using cloud-based backup or storage services (such as, e.g., Dropbox, Sugarsync, Apple's iCloud, or Google Drive) underscores the point. Thirty-five years ago, when the Supreme Court decided *Smith v. Maryland*, personal computers were in their infancy, mobile phones were almost unknown, and the word "cloud" usually referred only to the weather. In 2014, it is unlikely Americans would believe they have no privacy interest in documents stored on cloud servers, regardless of the so-called "third-party disclosure" doctrine purportedly derived from *Smith*. A fundamental difference between now and the late 1970s is that privacy policies are now ubiquitous and spell out in detail what a service provider (such as a telephone company or a cloud-storage provider) may and may not do with user data. The privacy policies provide individuals with an expectation that they have a level of control over information stored by a third party that likely never even occurred to people 35 years ago.

*ler* is an absolute bar to a reasonable expectation of privacy in anything a person does not keep absolutely secret. That is not the law. First, the Supreme Court itself does not consider the "doctrine" absolute. In the *Ferguson* case, for example, the Supreme Court concluded a Government program in which a hospital tested pregnant women's urine samples for drug use and then reported positive tests to the police was an unreasonable search prohibited by the Fourth Amendment. *Ferguson v City of Charleston*, 532 U.S. 67, 84–86 (2001).[33]

Second, decisions such as *Smith* and *Miller* have not overturned precedents such as *Stoner v. California*, 376 U.S. 483, 487–89 (1964) (recognizing hotel guest's right to control room and exclude police from searching even when he was not in room, notwithstanding fact that maids or repairmen might enter room without his knowledge). *Cf. O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) (recognizing, post-*Smith*, potential for government employee to have reasonable expectation of privacy in his workspace even though other people may have frequent access to it); *Randolph*, 547 U.S. at 106 (holding, post-*Smith*, that one occupant of shared residence may not consent to search over objection of co-resident who is present and voices objection); *see also Douglas v. Dobbs*, 419 F.3d 1097, 1102 (10th Cir. 2005) (finding, post-*Smith*, reasonable expectation of privacy in prescription drug records in hands of third party).

Third, courts have rejected the Government's theory that just because something is visible to the public automatically removes any expectation of privacy. *See Bond v. United States*, 529 U.S. 334, 336–38 (2000) (rejecting Government's argument that bus passenger loses expectation of privacy in carry-on bag placed on overhead rack where other people may touch it); *U.S. DoJ*, 489 U.S. at 770 ("In sum, the fact that an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information. The privacy interest in a rap sheet is substantial. The substantial character of that interest is affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten ….") (internal quotation marks and citation omitted);

[33] The Court reached this conclusion over Justice Scalia's dissenting argument that the "third-party disclosure" principle permitted the search. *Id.* at 95 (Scalia, J., dissenting).

*Maynard*, 615 F.3d at 559 ("[W]e ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do.").

Fourth, courts have also recognized that society recognizes the reasonableness of an implied contract between a business and its customers whereby the customers are entitled to expect the business will not disclose personal data to others and will take reasonable measures to protect the information. *See, e.g.*, *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 159 (1st Cir. 2011) ("The district court correctly concluded that a jury could reasonably find an implied contract between Hannaford and its customers that Hannaford would not use the credit card data for other people's purchases, would not sell the data to others, and would take reasonable measures to protect the information. … Ordinarily, a customer does not expect—and certainly does not intend—the merchant to allow unauthorized third-parties to access that data."); *In re Michaels Stores PIN Pad Litig.*, 830 F. Supp. 2d 518, 531 (N.D. Ill. 2011) (finding *Anderson*'s reasoning persuasive); *Claridge v. RockYou Inc.*, 785 F. Supp. 2d 855, 865 (N.D. Cal. 2011) (finding breach of contract claim viable when plaintiff alleged defendant failed to secure private data, such as e-mail addresses, passwords, and login credentials for social networks like MySpace and Facebook, from hackers). It is true these "implied contract" cases did not hinge on Fourth Amendment issues. However, it is also true that an *implied contract* between a business and its whole customer base is arguably a stronger indicator of what society (in the guise of the "reasonable man") expects as opposed to an express contract that may reflect the particular parties' unique requirements.

Fifth, while the Government devotes much effort to, essentially, arguing a motion for reconsideration of this Court's *Klayman* opinion, this Court did not act uniquely in *Klayman* by finding *Smith* and *Miller* inapposite. Other federal courts have likewise found mobile phone technology cases to be distinguishable from *Smith* and *Miller*. *See, e.g., In re Application of U.S. for Order Directing Provider of Elec. Commc'n Servs. to Disclose Records*, 620 F.3d 304, 317–19 (3d Cir. 2010) (rejecting Government's citation of *Smith* and *Miller* and finding "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way"); *In re Application of U.S. for Order Authorizing Disclosure of Location*

*Info. of Specified Wireless Telephone*, 849 F. Supp. 2d 526, 538 n.6 (D. Md. 2011) (relying on the Third Circuit's opinion "given the ubiquity of cellular telephones in modern American society"); *In re Application of U.S. for Order Authorizing Release of Historical Cell-Site Info.*, 736 F. Supp. 2d 578, 582 (E.D.N.Y. 2010) ("[I]t is no longer enough to dismiss the need for [constitutional] analysis by relying on cases such as *Knotts* or … *Smith* ….").

Finally, *Smith* itself has been substantively cited[34] in only *three* majority Supreme Court opinions over the years, and most recently in 1988. All three citations were for the proposition that recording phone numbers dialed through a pen register does not violate the Fourth Amendment. *See California v. Greenwood*, 486 U.S. 35, 41 (1988); *United States v. Jacobsen*, 466 U.S. 109, 122–23 n.22 (1984); *United States v. Knotts*, 460 U.S. 276, 283 (1983). Supreme Court case law thus does not support the talismanic effect the Government assigns to *Smith*.

### 3. The Supreme Court's *Jones* Analysis Subsequent to *Knotts* Supports the Conclusion That *Smith* Is Not Controlling in Light of Its Dissimilarity to the Present Case.

In *Knotts*, government officers installed an electronic beeper, which emitted signals that could be picked up by a radio receiver, inside a container of chloroform. When a codefendant purchased the chloroform, the officers followed the car in which the container had been placed, maintaining contact by using both visual surveillance and a monitor that received the radio signals sent from the beeper. Through the use of the beeper, the officers ultimately traced the chloroform to the location of the defendant's cabin. 460 U.S. at 277–79. Because all the tracking took place on public roads or in an open field, the Court held there was no reasonable expectation of privacy violated by tracking the beeper, and thus no Fourth Amendment search. *Id*. at 282.

The *Knotts* defendants were surveilled—with the aid of an electronic tracking device—for the duration of one trip. In *Jones*, however, the police placed a GPS tracking device on defendant's vehicle without a warrant and thereby tracked defendant's movements for *28 days*. The Government relied on *Knotts*, but the *Jones* Court held that, under a trespassory theory, the phys-

[34] "Substantively cited" means cited for a proposition uniquely derived from that opinion, as opposed to a routine phrase, such as "reasonable expectation of privacy."

ical placement of the GPS device and the use of that device to track the defendant constituted an unreasonable search in violation of the Fourth Amendment, and that such conclusion was all that was needed to decide the case. *Jones*, 132 S. Ct. at 951–52 (opinion of the Court) and 955 (Sotomayor, J., concurring). However, two concurrences totaling five Justices[35] stated that the *physical trespass* qua *physical trespass* to Jones's vehicle accomplished by placing the GPS tracking device directly thereon was not necessary to find an unconstitutional search under the "reasonable expectation of privacy" test derived from *Katz v. United States*, 389 U.S. 347 (1967).

The concurrences noted that "physical intrusion is now unnecessary to many forms of surveillance." *Id.* at 955 (Sotomayor, J., concurring),[36] 961–63 (Alito, J., concurring in judgment). All five concurring Justices concluded the extended, intimate electronic tracking of the defendant was by itself enough to find both an invasion of a reasonable expectation of privacy, and that a Fourth Amendment search had occurred. *Id.* at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring). The intrusiveness of extended electronic monitoring was deemed by the five concurring Justices to be a violation of Jones's reasonable expectations of privacy even though Jones was tracked traveling on public roads in a similar manner to the co-defendant in *Knotts*. Moreover, the five concurring Justices concluded that non-trespassory electronic surveillance violated reasonable expectations of privacy after *only 28* days of monitoring; whereas, in the case at bar the Government has been monitoring Plaintiffs for well *over 2800* days.

In *Smith*, a robbery victim described the defendant (Smith) and had suffered telephone harassment from the purported robber after the robbery. Smith's car was spotted in her neighborhood at the time of the robbery, thereafter, and in association with one of the harassing telephone

---

[35] Justice Sotomayor signed onto Justice Scalia's majority opinion and wrote a concurring opinion of her own. Justice Alito wrote an opinion concurring only in the judgment, joined by Justices Ginsburg, Breyer, and Kagan. Where Justice Sotomayor concluded that Jones's Fourth Amendment rights were violated both under a trespass theory and by violation of his reasonable expectations of privacy, *Jones*, 132 S. Ct. at 954–55 (Sotomayor, J., concurring), Justice Alito rejected the trespass theory and rested solely on the violation of Jones's privacy, *id.* at 957–58 (Alito, J., concurring in judgment).

[36] Justice Sotomayor went on to note that "[w]ith increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or *GPS-enabled smartphones*." *Id.* at 955 (Sotomayor, J., concurring) (emphasis added).

calls. Once police connected Smith to the car observed in the victim's neighborhood, they placed a pen register on his phone line at the phone company's central office without a warrant to determine if he was in fact the phone harasser and therefore likely the robber. *Smith*, 442 U.S. at 737. Smith was surveilled via the pen register for two days, and the Court concluded that "under these circumstances"—i.e., all the circumstances of a robber and a telephone harasser—there could be no reasonable expectation of privacy in the phone numbers Smith dialed. In the case at bar, millions of individuals Defendants acknowledge to be innocent of suspicion for *anything* have been surveilled for over 2,909 days as of the filing of this brief.[37] The means used for Defendants' surveillance of Plaintiffs in this case are so far beyond what was imaginable to the *Smith* Court as to make the difference between *Knotts* and *Jones* look infinitesimal. Given the different course the Supreme Court took in *Jones* as compared to *Knotts*, the same difference in direction should occur in this case as compared to *Smith*, and Defendants' Motion to Dismiss should be denied.

#### 4. If the Court Concludes *Smith v. Maryland* Dictates Dismissal of Plaintiffs' Claims, *Smith*'s Holding Should Be Revisited.

For the reasons stated above and in this Court's opinion in *Klayman*, the differences between the current NSA data collection program and the simple pen register at issue in *Smith* lead to the conclusion that *Smith* is not determinative of this case. However, if the Court finds *Smith* dispositive of Plaintiffs' claims, *Smith*'s holding should be revisited.[38]

*Smith*'s conclusion that the Fourth Amendment did not protect the telephone numbers of a person called from warrantless collection by the Government was at least partially premised on the Court's conclusions that "it is too much to believe that telephone subscribers … harbor any general expectation that the numbers they dial will remain secret …," *Smith*, 442 U.S. at 743, and any such "expectation is not one that society is prepared to recognize as reasonable." *Id*. (cita-

[37] Measured from June 1, 2006, until May 19, 2014.

[38] The Supreme Court reserves for itself "the prerogative of overruling its own decisions." *Rodriguez de Quias v. Shearson/Am. Express, Inc.*, 490 U.S. 477, 484 (1989). Plaintiffs raise this argument solely to preserve a challenge to *Smith*'s holding in the event a court finds *Smith* requires the dismissal of Plaintiffs' claims.

tion and internal quotation marks omitted). Plaintiffs aver the *Smith* Court's premises were incorrect. However, to the extent the *Smith* Court's premises may in fact have been correct in 1979, they are demonstrably incorrect now.

Plaintiffs and the American people as a whole today clearly believe they have a Fourth Amendment privacy interest in the metadata their telephones create, and therefore, the *Smith* holding rests on faulty premises.[39] Thus, to the extent *Smith* precludes the relief sought by plaintiffs here, it should be reversed.

## IV. PLAINTIFFS' METADATA HAS BEEN BOTH SEIZED AND UNREASONABLY SEARCHED BY DEFENDANTS UNDER THE MATP.

As a general rule, warrantless searches and seizures are *per se* unreasonable under the Fourth Amendment unless they fall within certain narrow exceptions to the general rule. *Nat'l Fed'n of Fed. Emps.—IAM v. Vilsack*, 681 F.3d 483, 488–89 (D.C. Cir. 2012). To be reasonable under the Fourth Amendment, a search or a seizure must normally be based on an individualized suspicion of wrongdoing. *Chandler v. Miller*, 520 U.S. 305, 313 (1997). Here, the Government does not attempt to argue that an individualized suspicion of wrongdoing exists and does not ad-

[39] Examples of states that have rejected *Smith* explicitly, and its corollary case regarding bank records (*United States v. Miller*, 425 U.S. 435 (1976)), *see generally People v. Mejia*, 157 Cal. Rptr. 233, 237 (Cal. App. 2d Dist. 1979) (finding a reasonable expectation of privacy in telephone records under the California Constitution); *Burrows v. Superior Ct.*, 529 P.2d 590 (Cal. 1974) (bank records); *State v. Thompson*, 760 P.2d 1162, 1167 (Idaho 1988) ("Perhaps the day will come when a majority of the United States Supreme Court will decide to overrule *Smith* and establish for the nation the protection to which we believe those who use telephones in Idaho are entitled. Until then, art. 1, § 17 will stand as a bulwark against the intrusions of pen registers into our daily life in Idaho."); *State v. McAllister*, 875 A.2d 866, 875 (N.J. 2005) ("Further, the advent of modern technology, coupled with the ubiquity of commercial banking, underscores both the ability of prying government eyes to obtain bank records and the need to protect ordinary citizens' financial privacy …."); *People v. Mason*, 989 P.2d 757, 759–60 (Colo. 1999) ("recognizing a privacy interest in telephone and bank records" under Colorado's state constitution); *Charnes v. DiGiacomo*, 612 P.2d 1117, 1121 (Colo. 1980) ("bank transactions are not completely voluntary because bank accounts are necessary to modern commercial life"); *Commonwealth v. DeJohn*, 403 A.2d 1283, 1291 (Pa. 1979) (finding a legitimate expectation of privacy in bank records under the Pennsylvania Constitution); *Winfield v. Div. of Pari-Mutuel Wagering*, 477 So. 2d 544, 546–48 (Fla. 1985) (bank records); *People v. Jackson*, 452 N.E.2d 85, 89 (Ill. App. 1st Dist. 1983) (bank records) ("Since it is virtually impossible to participate in the economic life of contemporary society without maintaining an account with a bank, opening a bank account is not entirely volitional and should not be seen as conduct which constitutes a waiver of an expectation of privacy"); *id.* at 88 ("[Other states] rejected the rationale in *Miller* because it relies for its analysis of an expectation of privacy upon the ownership and possession of the records and not the reasonable expectations of the individual.").

dress the MATP constituting an ongoing seizure of telephone metadata. Rather, the Government relies on the argument that its conduct is justified by "special government needs." As demonstrated below, the Government is wrong.

### A. Defendants' Interference with Plaintiffs' Possessory Interest in Their Metadata Constitutes a Seizure Because It Eliminates Plaintiffs' Contractual Possessory Rights in Their Metadata.

As previously discussed, Plaintiffs have established control over their metadata due to their contracts with their phone companies.

"A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). This applies to both physical property, such as a house or car, and intangible matter, such as electronic data: "[I]t is clear that … the Fourth Amendment extend[s] to searches for and seizures of intangibles …." *United States v. Villegas*, 899 F.2d 1324, 1334–35 (2d Cir. 1990) (noting "seizure of intangible evidence has been explored principally in the context of the interception of communications"). The Government's taking of computer or mobile-phone data constitutes a "seizure" for Fourth Amendment purposes. *In re Search of Apple iPhone*, Mag. Case No. 14-278 (JMF), 2014 WL 1239702, at **4–5 (D.D.C. Mar. 26, 2014) (Facciola, Mag. J.) (referring multiple times to government "seizure" of data).

"One of the main rights attaching to property is the right to exclude others, and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude." *Rakas*, 439 U.S. at 143 n.12 (citing Blackstone's Commentaries, Book 2, ch. 1). In this case, Plaintiffs' contracts with the telephone companies preserve their right to exclude others from viewing their metadata. The MATP does not merely *interfere* with Plaintiffs' possessory right to exclude others from viewing their metadata. It completely *eliminates* that right.

As a Magistrate Judge of this Court recognized earlier this year, it is constitutionally unacceptable for the Government to make a copy[40] of a full set of data that includes data the Government has no probable cause to seize and then to maintain that copy for some lengthy indefinite period of time. *In re Search of iPhone*, 2014 WL 1239702, at *5; *see also United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) (condemning "the wholesale seizure for later detailed examination of records not described in a warrant"); *cf. United States v. Saboonchi*, No. PWG-13-100, 2014 WL 1364765, at *26 (D. Md. Apr. 7, 2014) (Grimm, J.) ("… [T]he government cannot simply seize property under its border search power and hold it for weeks, months, or years on a whim.") (internal quotation marks omitted) (quoting *House v. Napolitano*, No. 11-10852-DJC, 2012 WL 1038816, at *9 (D. Mass. Mar. 28, 2012)). Contrary to the Government's assertion that "container" cases control (*see* Gov't Br. at 24 & n.11, 35–36), this case does not involve a situation where the Government seizes something contained in a box or other storage medium and then holds onto it without using it. In this case, there is no "container." Either the Government obtains the telephone metadata and adds it to its database or it does not. The Government admits it does obtain the data. (*See* Gov't Br. at 6.) As discussed below, the Govern-

[40] For purposes of a Fourth Amendment seizure analysis, it is immaterial that the government requires phone companies to produce electronic copies of telephone metadata rather than mandating they hand over "original" data and then wipe it from their systems. While in the context of physical property courts traditionally believed no "seizure" occurred unless the government's action ousted the owner from actual control of property, computer data (including telephone metadata) is different. As the Supreme Court has recognized in the context of audio recordings of attorney-client conversations, "even if the Government retains only copies of the disputed materials, a taxpayer still suffers injury by the Government's continued possession of those materials, namely, the affront to the taxpayer's privacy." *Church of Scientology of Cal. v. United States*, 506 U.S. 9, 13 (1992). The same principle should apply in the context of electronic data. "An image of an electronic document contains all of the same information as the original electronic document. To the extent the owner or custodian of the electronic document has privacy concerns regarding the government's retention of the original document, the owner would have identical privacy concerns with the government's retention of the imaged document." *United States v. Metter*, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012). Put differently, when the government seizes an electronic storage device to search the data stored thereon, the government's primary interest is not really in the physical device itself but rather in whatever is stored on that device. (The same is true, of course, of paper documents: Normally it is not the actual piece of paper that is of interest but the information on the piece of paper.) If the user has a privacy interest in excluding other people from viewing the data on his device, there is no reason why a different rule should apply to a copy of that data.

ment's action in obtaining the metadata and adding it to the database constitutes not only a seizure, but essentially an instantaneous search.

Finally, the MATP also constitutes a seizure because it represents the Government taking control of data so as to be able to search it at any time. Even if it were true, as the Government contends, that no individual can know whether the Government has conducted any searches relating to a specific phone number, and even if it were true that a particular phone number has not been the subject of any such search (points Plaintiffs do not concede), the MATP still involves the Government acquiring daily metadata records from Plaintiffs' telephone companies and integrating them into a pre-existing database so they can be accessed at any time. In other words, for purposes of assessing whether a Fourth Amendment "seizure" has occurred, it is irrelevant whether the Government actually searches the materials it seizes. *Cf. Metter*, 860 F. Supp. 2d at 215 ("The parties have not provided the Court with any authority, nor has the Court found any, indicating that the government may seize and image electronic data and then retain that data with no plans whatsoever to *begin* review of that data to determine whether any irrelevant, personal information was improperly seized. The government's blatant disregard for its responsibility in this case is unacceptable and unreasonable.") (italics in original).

### B. The MATP Constitutes an Ongoing Unreasonable Search of Plaintiffs' Metadata.

The Fourth Amendment prohibits "unreasonable searches and seizures." U.S. Const. amend. IV. An analysis of whether a search violates the Fourth Amendment therefore requires a determination of (1) whether a "search" has occurred for purposes of the Fourth Amendment and, if so, (2) whether it is "reasonable" within the Fourth Amendment's meaning, including whether it falls within an exception to the general rule that warrantless searches not based on an individualized suspicion of wrongdoing are *per se* unreasonable. *Kyllo*, 533 U.S. at 31.

#### 1. The MATP Constitutes a Search.

"When the Fourth Amendment was adopted, as now, to 'search' meant '[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search*

the house for a book; to *search* the wood for a thief." *Kyllo*, 533 U.S. at 32 n.1 (quoting Webster, *An American Dictionary of the English Language* 66 (1828) (reprint 6th ed. 1989)). A "search" occurs for purposes of the Fourth Amendment when the Government either (a) "obtains information by intruding on a constitutionally protected area," *Jones*, 132 S. Ct. at 950 n.3, or (b) "violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo*, 533 U.S. at 33 (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)); *see also Jacobsen*, 466 U.S. at 113 ("A 'search' occurs when an expectation of privacy that society is prepared to recognize as reasonable is infringed."). In this case, the Government has not intruded on constitutionally-protected physical space; the question is whether the Government is violating Plaintiffs' reasonable expectation of privacy by collecting their telephone metadata with no individual suspicion of wrongdoing and then retaining and analyzing that metadata for years.

The crucial test is whether *American society* recognizes the expectation of privacy as reasonable. The Government gives *Smith v. Maryland* almost talismanic effect, but *Smith*, even if correctly decided, cannot establish whether society reasonably expects that the current scope and type of metadata collected is deserving of privacy protections. Neither American society nor the Supreme Court in 1979 could have anticipated the scope and breadth of 21st-century cell phones and the information they contain and generate, and, therefore, neither developed any expectation *then* regarding whether the *current* searches and seizures are reasonable. While the concept of the privacy interest the Fourth Amendment protects dates to 1792, determining society's reasonable expectation regarding devices and information that were unimaginable in 1792 (and in 1979 for that matter) necessarily requires the Court turn to current societal views. For the reasons stated previously, there is no question that contemporary American society has an expectation that this information is private, and such an expectation is objectively reasonable.[41]

[41] This also shows the error of the government's assertion in footnote 16 of its brief (page 30) that public opinion polls and actions of state legislatures are irrelevant. To the contrary, such evidence is *extremely relevant and compelling* as to whether society believes an expectation of privacy is reasonable. *Cf. Maynard*, 615 F.3d at 564 ("Although perhaps not *conclusive* of nationwide 'social understandings,' these state laws are indicative that prolonged GPS monitoring defeats an expectation of privacy that our society

The Government also argues (Br. at 32–33) that if a "search" occurs, it occurs only when an NSA analyst reviews the results of a query of the Government's database of call detail records. The Government is wrong. A search is a search regardless of whether a human combs through boxes of documents or whether a computer is used to automate the process.[42] Every time the Government uses a "seed" to query the database, it must search the entire database—otherwise, there would be no way to know whether the process detected all numbers within two "hops." The computer's action in selecting or rejecting particular numbers constitutes a "search" because it performs the essential function of pre-screening the data the NSA analyst sees.

For the reasons previously discussed, Plaintiffs have an expectation of privacy in their metadata and American society recognizes that expectation as reasonable. Therefore, the MATP constitutes a "search" for purposes of the Fourth Amendment.

### 2. The MATP Is an Unreasonable Search Because the Government Cannot Demonstrate "Special Needs."

As noted above, the general rule is that warrantless searches and seizures are *per se* unreasonable under the Fourth Amendment unless they fall within certain narrow exceptions to the general rule. *IAM*, 681 F.3d at 488–89. To be reasonable under the Fourth Amendment, a search or a seizure must normally be based on an individualized suspicion of wrongdoing, *Chandler*, 520 U.S. at 313, or else it must fall within one of the "few specifically established and well-delineated exceptions to that general rule" recognized by the Supreme Court. *IAM*, 681 F.3d at 489 (quoting *City of Ontario v. Quon*, 130 S. Ct. 2619, 2630 (2010)).

In this case, the Government cites—in a surprisingly cursory argument (Br. at 36–38)—what it views as the "special needs doctrine," arguing blanket suspicionless searches constitute a reasonable infringement on privacy rights if the Government has "special needs" allegedly compelling a search. Essentially, the Government contends thwarting terrorist attacks is a vital gov-

---

recognizes as reasonable. So, too, are the considered judgments of every court to which the issue has been squarely presented.") (emphasis supplied and citation omitted).

[42] Ironically, in *Smith v. Maryland* itself, the Court refused to distinguish between actions taken by a human telephone operator versus actions taken by automated switching equipment. 442 U.S. at 744–45.

ernment interest justifying blanket suspicionless searches of the entire American population as a way to *develop* evidence, rather than as a *response* to evidence.[43] In other words, the ends justify the means. The Government also contends the MATP is justifiable because it is a *faster way* to develop evidence than other methods. Oddly, the Government makes no serious argument and merely states the MATP "clearly serves special government needs." (Gov't Br. at 37.)

The Court should reject the Government's *ipse dixit* conclusion because the "special needs" case law does not support it and because the Government's position is backwards. It essentially says a search is *presumed reasonable* whenever the Government claims special needs, but federal courts have held warrantless searches are normally *presumed unreasonable* absent narrow and specific circumstances. The MATP does not fall within those circumstances.

"A search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing. While such suspicion is not an 'irreducible' component of reasonableness, we have recognized *only limited circumstances* in which the usual rule does not apply. For example, we have upheld certain regimes of suspicionless searches where the program was designed to serve 'special needs, beyond the normal need for law enforcement.'" *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000) (citations omitted and emphasis supplied).[44] The *Edmond* Court cited several examples but, notably, cautioned, "In none of these cases … did we indicate approval of a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing." *Id.* at 38.[45] "Even where the government claims 'special needs,' a warrantless search *is generally unreasonable* unless based on 'some quantum of individualized suspicion.'"

---

[43] Plaintiffs strongly believe fighting terrorism is a critical role of government.

[44] As examples of such permissible suspicionless searches, the Court cited *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995) (random drug testing for student athletes); *Treasury Emps. v. Von Raab*, 489 U.S. 656 (1989) (drug tests for certain Customs employees); *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602 (1989) (drug and alcohol tests for railway employees); *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976) (searches by the Border Patrol); *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444 (1990) (DUI checkpoints); and *Delaware v. Prouse*, 440 U.S. 648 (1979) (in which the Court *suggested*, but did not hold, that license-and-registration checkpoints *might* be permissible in certain situations).

[45] *Cf. also Illinois v. Lidster*, 540 U.S. 419, 424–27 (2004) (finding a police roadblock constitutional where the purpose "was to help find the perpetrator of a specific and known crime, not unknown crimes of a general sort[,]" by asking motorists if they knew anything about a prior hit-and-run accident).

*IAM*, 681 F.3d at 489 (emphasis supplied) (quoting *Skinner*, 489 U.S. at 624); *see also Lidster*, 540 U.S. at 426 (noting presence of "special needs" "***does not*** mean the [search] is automatically, or even presumptively, constitutional. It simply means that we must judge its reasonableness, hence its constitutionality, on the basis of the individual circumstances.") (emphasis supplied).

A court may not simply accept the Government's invocation of the words "special needs" and instead must conduct a "close review" of the scheme in question, *Ferguson*, 532 U.S. at 81 (citing *Chandler*, 520 U.S. at 322), while being mindful that "the gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement officers may use to pursue a given purpose." *Edmond*, 531 U.S. at 42; *see also Maryland v. King*, 133 S. Ct. 1958, 1970 (2013) ("Urgent government interests are not a license for indiscriminate police behavior."). Thus, a court considering a "special needs" claim must "balance the individual's privacy expectations against the government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context," and the court must "undertake a context-specific inquiry, examining closely the competing private and public interests advanced by the parties." *IAM*, 681 F.3d at 489 (quoting *Von Raab*, 489 U.S. at 665–66, and *Chandler*, 520 U.S. at 314). The court must consider "the nature of the privacy interest allegedly compromised," "the character of the intrusion imposed," and "the nature and immediacy of the government's concerns and the efficacy of the [p]olicy in meeting them." *Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls*, 536 U.S. 822, 830–34 (2002).

In this case, Plaintiffs have established the reasonableness of their significant interest in maintaining the privacy of their telephone metadata, and it is unquestionable the MATP intrudes upon that interest.[46] The remaining factor—the nature and immediacy of the Government's concerns and the efficacy of the MATP in meeting them—tips strongly in favor of Plaintiffs.

First, while Plaintiffs do not dispute the importance of identifying terrorist operatives and preventing terrorist attacks, such an interest does not justify a secret blanket warrantless search

[46] The government does not seriously argue the MATP does not intrude on the privacy of telephone metadata, and simply maintains there is no reasonable expectation of privacy in that information.

of all telephone metadata from all (or substantially all) American citizens. The *Edmond* Court noted "the Fourth Amendment would *almost certainly* permit *an appropriately tailored road-block set up to thwart* ***an imminent terrorist attack***." 531 U.S. at 44 (emphasis supplied).[47] The word "imminent" is critical. Its primary definition is "[o]f an event, esp. danger or disaster: *impending, soon to happen.*" 1 SHORTER OXFORD ENGLISH DICTIONARY 1323 (5th ed. 2002) (emphasis supplied). That is, in such a scenario the Government would already have compelling evidence showing a particular terrorist attack is likely to happen in the near future (as opposed to the general mantra "terrorists are looking to strike the United States")—the existing evidence obtained through proper methods would be the *basis* for claiming the "special need." But in this case, the Government is attempting to invert the process—the Government has no evidence and instead seeks to cull through massive amounts of data attempting to ferret out terrorism.

Thus, the alleged "special need" is the Government's desire to seek evidence, which may or may not exist, regarding unknown hypothetical terrorist attacks. The "nature and immediacy" of the Government's concerns do not justify the MATP because it is not based on thwarting an "imminent" attack. *Cf. Chandler*, 520 U.S. at 318–19 ("Notably lacking in respondents' presentation is any indication of a concrete[48] danger demanding departure from the Fourth Amendment's main rule."); *Ferguson*, 532 U.S. at 83 & n.21 (rejecting "special needs" argument where "the immediate objective of the searches was to generate evidence for law enforcement purposes" (emphasis removed) and noting that "[i]n none of our previous special needs cases have we upheld the collection of evidence for criminal law enforcement purposes."); *Edmond*, 531 U.S. at 42 (expressing concern at the specter of allowing searches "for almost any conceivable law enforcement purpose" such that "the Fourth Amendment would do little to prevent such intrusions from becoming a routine part of American life.").

---

[47] The Court also posited using roadblocks to "catch a dangerous criminal who is likely to flee by way of a particular route," *id.*, again envisioning a scenario where evidence already exists.

[48] While not exactly synonymous with "imminent," the word "concrete" as used by the *Chandler* Court has a similar sense in that it refers to something specific or definite. 1 SHORTER OXFORD ENGLISH DICTIONARY 478 (column 1, definition 3).

Second, the Government has been unable to cite to a single example of the MATP stopping an "imminent" terrorist attack or aiding in the accomplishment of any urgent objective. In fact, three members of the U.S. Senate Select Committee on Intelligence—who have access to classified information about Government surveillance efforts that is not available to the public—have stated that "[a]s members of the committee charged with overseeing the National Security Agency's surveillance, [they] have reviewed this surveillance extensively and have seen no evidence that the bulk collection of Americans' phone records has provided any intelligence of value that could not have been gathered through less intrusive means."[49] Notably, the senators contend the Government's claim the MATP has helped "thwart" or "disrupt" 54 specific terrorist plots **is untrue** because the MATP played little or no role in all but two of them, and even in those two cases the information "could readily have been obtained without a database of all Americans' call records."[50] Thus, they conclude "there appears to be nothing uniquely valuable about the program, and … existing alternative legal authorities are sufficient to accomplish the United States' legitimate intelligence objectives without systematically infringing on the privacy rights of hundreds of millions of Americans.[51]

Third, when the Government asked the FISC to authorize the MATP, the Government lied about its importance to counterterrorism efforts and failed to disclose other efforts then underway. In March 2009, the FISC noted that

> nearly all of the call detail records collected pertain to communications of non-U.S. persons who are not the subject of an FBI investigation to obtain foreign intelligence information, are communications of U.S. persons who are not the subject of an FBI investigation to protect against international terrorism or clandestine intelli-

[49] Brief of *Amici Curiae* Senators Ron Wyden, Mark Udall, and Martin Heinrich in Support of Plaintiffs, *First Unitarian Church of L.A. v. Nat'l Security Agency*, No. 3:13-cv-03287-JSW, at 2 (N.D. Cal.), Docket Entry 63-2 (filed Nov. 18, 2013) (hereinafter "Senators' Brief"). Similar to the manner in which a privilege log describes attorney-client communications without divulging their substance, the Senators' Brief discusses the MATP without divulging classified information.

[50] *Id.* at 6–7.

[51] *Id.* at 13–14. The senators also noted that, while the government claims 12 other examples show the MATP's value, their review of those examples revealed the government's description was exaggerated.

> gence activities,[52] and are data that could not otherwise be legally captured in bulk by the government. *Ordinarily, this alone would provide sufficient grounds for a FISC judge to deny the application.*

*In re Production of Tangible Things from [Redacted]*, No. BR 08-13, slip op. at 12 (FISC Mar. 2, 2009) (underlining in original, italics supplied).[53] The court noted the Government had stated, under oath, that the collection of telephone metadata was "necessary," and elsewhere in the opinion the court noted the NSA claimed the collection of such data is "vital" and "[t]he only effective means by which NSA analysts" could perform certain functions. *Id.* at 2, 12, and 17..[54] The court found the Government's submissions regarding the value of the metadata program were of suspect value. *See id.* at 13; *see also* Senators' Brief, *supra*, at 7 ("In both public statements and in newly declassified submissions to the SSCI, intelligence officials have significantly exaggerated the phone-records program's effectiveness.").

Since those original submissions, however, the Government has backed off and now describes the MATP in hedged terms. In submissions to other courts, the Government has replaced words like "vital" and "only effective means" with language describing the program as "one method that the NSA has developed," a method that "can contribute to the prevention of terrorist attacks," and "a tool for detecting communications chains." Jaffer, J., *The Basis for the NSA's Call-Tracking Program Has Disappeared, If It Ever Existed* (Nov. 7, 2013).[55] In this case, the Government asserts thwarting terrorism "cannot be as effectively achieved" through use of constitutional methods for gathering information. (Gov't Br. at 38). "Cannot be as effectively achieved" is an obvious hedge—in other words, "we could still do it but with more effort." Thus, the FISC's suspicions in March 2009 were well-founded, as the Government no longer character-

---

[52] In other words, data regarding American citizens is collected with no individualized suspicion of wrongdoing.

[53] As of March 21, 2014, available at https://ia601003.us.archive.org/25/items/785247-march22009orderfromfiscnsasurveillance/785247-march22009orderfromfiscnsasurveillance.pdf.

[54] The description of these functions was redacted when the opinion was declassified.

[55] As of April 22, 2014, available at http://justsecurity.org/2013/11/07/basis-nsas-call-tracking-program-disappeared-existed/. The dramatic shift in the Government's language from 2009 to today suggests that when they originally testified before the FISC, Government personnel never though their apocalyptic testimony would be become public.

izes the MATP as indispensable. Moreover, if the Government itself concedes the program is not "vital," it seriously undercuts the "special needs" argument.[56]

Finally, even if the MATP might be a "more efficient" way for the Government to obtain telephone metadata about persons of interest than the use of warrants based on individual suspicion, that is not enough to make it lawful.[57] "The 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 (suggesting while police could lawfully observe a house to find out how many people live there, "that does not make breaking and entering to find out the same information lawful").

Thus, the MATP violates the Fourth Amendment because it constitutes an impermissible seizure and an unreasonable search.

## V. THE FOURTH AMENDMENT PRESERVES THE DEGREE OF PRIVACY AGAINST GOVERNMENT THAT EXISTED WHEN THE AMENDMENT WAS RATIFIED.

For over a decade, the Supreme Court has explicitly noted that the Fourth Amendment "'assur[es] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Jones*, 132 S. Ct. at 950 (five-justice majority) (quoting

---

[56] Notably, in March 2014 the public learned the NSA "has built a surveillance system capable of recording '100 percent' of a foreign country's telephone calls, enabling the agency to rewind and review conversations as long as a month after they take place." Gellman & Soltani, "NSA Surveillance Program Reaches 'into the Past' to Retrieve, Replay Phone Calls," Wash. Post (Mar. 18, 2014), *available at* http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (accessed Mar. 21, 2014). In other words, the system allows the NSA to "swallow[ ] a nation's telephone network whole." *Id.* (At the government's request, the *Washington Post* withheld details that could be used to identify the country as to which the system is in use and other countries for which its use is being considered.) Thus, even if at one time the MATP may have been "vital" or "the only effective means" to certain ends (a contention Plaintiffs dispute), clearly that is no longer the case. If government surveillance of foreign communications reveals something of national security interest, the government will have the evidence needed to obtain either a warrant or other legal authority allowing it to investigate further as to specific American phone numbers that had been in contact with the foreign number in question—i.e., there would be "some quantum of individualized suspicion," *IAM*, 681 F.3d at 489 (quoting *Skinner*, 489 U.S. at 624).

[57] *Cf.* Senators' Brief, *supra*, at 8–11 (discussing alternative legal authorities via which the government could have "simply obtained … information from phone companies using more calibrated legal instruments" rather than bulk data collection).

*Kyllo*, 533 U.S. at 34) (second bracket from *Jones*); *see also Jones*, 132 S. Ct. at 958 (Alito, J., concurring in judgment for the other four Justices). The Court, however, has not explained in detail what that commitment would look like applied to the mass collection of personal data. In *Jones*, Justice Alito noted that

> [i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources.

*Id.* at 963–64 (Alito, J., concurring in judgment) (citations omitted). Hence, while the Supreme Court has not yet had the opportunity to review today's mass data collection by the Government, it has instructed that such conduct be evaluated against the "degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* at 950 (opinion of the Court).

In 1792, the primary means of communication was also by mail instead of phone,[58] and the Founders were highly protective of its privacy, an approach that was nearly unique in the Western world at that time. Butschek, A., et al., *The Founding Fathers and the Fourth Amendment's Historic Protections Against Government Surveillance: A Historic Analysis of the Fourth Amendment's Reasonable Expectations of Privacy Standards as It Relates to the NSA's Surveillance Activities* at 4–5.[59] The Founders' concern for protecting the privacy of mail arose from their colonial experience, during which the British either inspected or blocked the delivery of mail as part of their intelligence and suppression efforts. *Id.* at 3–4.

---

[58] The comparison of telephone communication to mail was made by both the majority and the dissent in *Olmstead v. United States*, 277 U.S. 438 (1928). The majority declined—at that time—to give telephone communications the protections of mail because of the intangible nature of telephone communications, *id.* at 464, while the dissent argued that intangible telephonic communications deserve the same level of protection as that afforded to mail. *Id.* at 475. Of course, such protection was finally recognized as appropriate in *Katz* based upon the demonstrated and reasonable expectation of privacy of the target of the surveillance. *Katz*, 389 U.S. at 353 (explicitly overruling *Olmstead*).

[59] Available at https://www.rutherford.org/files_images/general/2014_Historic_4th_Amendment-NSA_Metadata.pdf (as of May 14, 2014).

With no universal addressing system in 1792,[60] identifying mail addresses with specificity would have required following a piece of mail to the last post office in the chain of post offices through which a letter passed. All the other postmasters along the way did nothing more than move the letter closer to its ultimate destination. *Id.* at 5–6 (citing John, R., *Spreading the News: The American Postal System from Franklin to Morse* at 74–75 (1998)). A typical address would be solely "name, title or profession, city." Thus, a letter could be addressed simply to "W. Henry, Esq., Hanover," and other than (hopefully) knowing where Hanover County, Virginia, was, the postmasters along the letter's route would do no more than move the letter on down the line, relying on the closest postmaster to get the letter to Mr. Henry, its intended recipient. *Id.* at 27.

Moreover, as Justice Alito observed in *Jones*, only the most important investigations received attention in the form of dedicated resources, thereby further affecting the reasonable expectation of privacy one would have had against government in 1792. *Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring in judgment). There were 17 federal statutory criminal offenses enacted in 1790,[61] and presumably a similar number by 1792, whereas today there are more than the federal government is able to count, though the most recent estimate from 2013 was approximately 4,500.[62] At the time the Fourth Amendment was ratified, law enforcement resources were neither applied nor even available to address crime or intelligence gathering. There were no full-time prosecutors or professional police forces.[63] Crime victims presented their own cases to courts until the late 19th century.[64] Until well into the 19th century, law enforcement officers did not take preventive actions to fight crime, but responded only after a crime had occurred.[65]

---

[60] With no standardization in addressing, there was no equivalent to telephone metadata in 1792.

[61] *See* Crimes Act of 1790, ch. 9, 1 Stat. 112. All other federal crimes were common law crimes, until 1812 when the Supreme Court held that there were not, in fact, any federal common law crimes. *United States v. Hudson & Goodwin*, 11 U.S. (7 Cranch) 32 (1812).

[62] Ruger, T., Way Too Many Criminal Laws, Lawyers Tell Congress, Blog of the *Legal Times* (June 14, 2013).

[63] Walker, S., *Popular Justice: A History of American Criminal Justice* at 25 & 29 (2d ed. 1998).

[64] *Id*. at 71.

[65] Lane, R., *Urban Police and Crime in Nineteenth-Century America*, 2 CRIME & JUSTICE 1, 4 (1980); Uchida, C., *The Development of the American Police: An Historical Overview* at 5 (Dec. 2004); and

In light of the postal system as it then existed in tandem with the complete lack of affirmative law enforcement or intelligence gathering in 1792, American citizens had very high expectations of privacy in their communications. Even if the federal government had been so inclined, the manpower required and the decentralization of letter delivery would have completely foreclosed anything analogous to the NSA's MATP. It would not just have been impossible in 1792, but it also would have radically violated individual Americans' privacy expectations at the time. Consistent with the rationale found in *Jones*, this Court should also find that the MATP falls not only below the level of privacy an American would have expected in 1792, but that it does so today as well.

## CONCLUSION

For all the foregoing reasons, the Court should decline to follow *Smith v. Maryland* and should deny the Government's Motion to Dismiss.

Respectfully Submitted,

/s/ Kenneth T. Cuccinelli
Kenneth T. "Ken" Cuccinelli, II (*admitted pro hac vice*)
KCuccinelli@CuccinelliAndAssociates.com
Cuccinelli & Associates, PLLC
10560 Main Street, Ste. 218
Fairfax, Virginia 22030

/s/ Earl "Trey" Mayfield
Earl "Trey" Mayfield (D.C. Bar # 459998)
tmayfield@lewis-firm.com
Michael P. Lewis (D.C. Bar. # 503311)
mlewis@lewis-firm.com
The Lewis Firm, PLLC
901 New York Ave., Ste. 450E
Washington, D.C. 20001
Tel: 202-630-6006
Fax: 888-430-6695
*Counsel for Plaintiffs*

---

Friedman, L., *Crime and Punishment in American History* at 204 (1993) (identifying the mid-19th century as the point in time when police departments first began formally investigating crimes).