U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2015 JUN -5 PM 1:37

LEEANN FLYNN HALL
CLERK OF COURT

IN THE UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT

Kenneth T. Cuccinelli, II, and FreedomWorks Foundation, Movants, v. President Barack Obama, Director of National Intelligence, James Clapper, Director of Federal Bureau of Investigation, James Comey, and Director of National Security Agency, Admiral Michael Rogers, Respondents.	)	FISC Case No.: 15-01

MOTION IN OPPOSITION TO GOVERNMENT'S IMMINENT OR RECENTLY-MADE REQUEST TO RESUME BULK DATA COLLECTION UNDER PATRIOT ACT §215

Movants come before this Court in accordance with Rule 6 of this Court asking to be heard in opposition to Respondents' (alternatively "the Government") necessary request for the re-institution or continuation of authority for the bulk collection of telephone metadata (hereafter "metadata collection") under Section 215 of the Patriot Act, 50 U.S.C. § 1861 (hereafter "Section 215"), as extended for 180 days by Section 109 of the recently-enacted USA Freedom Act of 2015 (hereafter "USA Freedom Act").

INTRODUCTION

SUBJECT MATTER JURISDICTION AND AUTHORITY TO GRANT RELIEF

This Court has subject matter jurisdiction over this Motion under 50 U.S.C. § 1803. This Court has authority to grant declaratory relief under the Declaratory Judgment Act, 28 U.S.C. §§ 2201-2202. This Court has authority to award costs and attorney's fees pursuant to 28 U.S.C. § 2412.

PERSONAL JURISDICTION AND VENUE

This Court possesses personal jurisdiction over the Respondents because of their filings in this Court on the subject matter of this Motion and as a result of this Court's nationwide

jurisdiction under the Patriot Act, including encompassing the actions of Respondents related to the subject matter of this Motion. Venue is proper in this Court for the foregoing reasons as well.

PARTICIPANTS IN THIS MOTION IN OPPOSITION

Movant and Counsel Kenneth T. Cuccinelli, II ("Cuccinelli") is a citizen of the United States and a resident of the Commonwealth of Virginia. Cuccinelli has standing to bring this Motion because Respondents have, without legitimate legal basis, seized, stored, retained, and periodically searched telephone metadata concerning virtually every domestic or international phone call he made or received since at least May 2006, and upon information and belief, Respondents seek to continue to do so. Cuccinelli uses and has used both cellular and/or landline telephones in the United States on a daily basis since May 2006, and he has been a subscriber of both cellular and landline telephone services since May 2006. Such telephone services have included, but not been limited to, Verizon Wireless, AT&T, and Comcast services. Movant has a subjective expectation of privacy from Respondents about his telephone metadata that society views as reasonable, and has property and contract rights in his telephone metadata that Respondents have violated and seek to continue to violate. Cuccinelli is an attorney in good standing with the Virginia State Bar, bar number 39,490. He is also an attorney in good standing of the bars of the following federal courts and agency: the United States Supreme Court, the Courts of Appeals for the Fourth and District of Columbia Circuits, the Federal District Courts for the Eastern and Western Districts of Virginia, the Court of International Trade, the Court of Appeals for Veterans Claims, and the U.S. Patent and Trademark Office (patent attorney). Cuccinelli is the former Attorney General of Virginia, in which capacity he held a Secret

Clearance until January 2014. Cuccinelli's other information required under Rule 7(h)(1) of the Rules of this Court may be found in the signature block of this Motion.

Movant FreedomWorks, Inc. is a not for profit Washington, D.C. corporation located at 400 North Capitol Street, N.W., Suite 765, Washington, D.C. 20001 ("FreedomWorks"). FreedomWorks has standing to bring this Motion because Respondents have, without legitimate legal basis, seized, stored, retained for five years, and periodically searched telephone metadata concerning every domestic or international phone call made or received by FreedomWorks, its employees conducting business on its behalf, and its members participating in its activities since at least May 2006, and upon information and belief, Respondents seek to continue to do so. FreedomWorks, its employees and members use both cellular and landline telephones in the United States, and FreedomWorks is a subscriber of both cellular and landline telephone services. FreedomWorks also funds the cellular telephone plans of many of its employees. Such telephone services have included, but not been limited to, Verizon Wireless and AT&T services. FreedomWorks (and its employees and members) has a subjective expectation of privacy from Respondents of its telephone metadata that society views as reasonable, and has property and contract rights in its telephone metadata that Respondents have violated and seek to continue to violate. Only the Chief Executive Officer of FreedomWorks, Adam Brandon, has knowledge of this Motion at the time of filing.

Movants Cuccinelli and FreedomWorks are situated similarly, and have similar interests, to the approximately 300 million other Americans who use cell phones and landlines.

Respondent Barack H. Obama is the President of the United States endowed with ultimate authority over each of the federal agencies relevant to this Motion.

Respondent James R. Clapper is the Director of National Intelligence endowed with ultimate authority over the activities of the intelligence community, including activities undertaken pursuant to Section 215 of the Patriot Act.

Respondent Admiral Michael Rogers is the Director of the National Security Agency ("NSA"), in the Department of Defense, and is Chief of the Central Security Service. Adm. Rogers has ultimate authority to supervise and implement all functions and operations of the NSA, the agency that has and upon information and belief seeks to continue to conduct the metadata collection under the auspices of Section 215. Adm. Rogers personally authorizes and supervises the metadata collection.

Respondent James B. Comey, Jr. is the Director of the FBI and is responsible for applications made to this Court for orders demanding the production of "tangible things" under Section 215, which is a cornerstone of the metadata collection.

Movants do not expect to object to the removal of Respondents determined to be unnecessary to the determination of this Motion, upon establishment thereof by this Court.

THIS MOTION IN OPPOSITION IS TIMELY IN LIGHT OF RECENT CIRCUMSTANCES

From May 2006 until May 31, 2015, Respondents conducted the metadata collection under a series of secret orders issued by this Court pursuant to Section 215. The authority for such orders, and the most recent order, expired at midnight, May 31, 2015. Two days later, Section 215 was reinstated by Congress and the President with an amendment blocking the metadata collection from continuing after 180 days, thereby suggesting Congress' agreement with the Second Circuit's recent ruling in *ACLU v. Clapper*, 2015 U.S. App. LEXIS 7531 *4 (2d Cir. May 7, 2015), in which that court held that the metadata collection was beyond the scope of Section 215. *See* USA Freedom Act, §§ 107 & 109.

Upon information and belief, all major telecommunications companies operating in the United States provided NSA on an ongoing daily basis telephone metadata for all telephone calls on their networks in, to or from the United States, including the calls of Movants.[1] Movants' metadata has been seized, maintained, and periodically searched in a single database without any specific belief by Respondents at the time of seizure, retention or searching that any of the information is connected with international terrorism or an international terrorist organization. Movants hold subjective expectations of privacy over their seized, retained, and searched telephone metadata, which expectations society views as reasonable; additionally, Movants have both property and contractual rights that have been violated by Respondents. Upon information and belief, the Respondents have applied to this Court, or shortly will apply, for the reinstatement of the aforementioned authority.

The intent to file such application by Respondents was publicly stated by the President in a statement upon signing the USA Freedom Act on Tuesday, June 2, 2015: "...my administration will work expeditiously to ensure our national security professionals again have the full set of vital tools they need to continue protecting the country." [2] Government officials clarified that such tools include renewal/re-institution of this Court's Section 215 order regarding metadata collection, and they estimated that the process would take "three or four days." *Id.*

---

[1] News reports immediately following the initial disclosure of the April 25, 2013 Verizon order, *In re Application of the FBI for an Order Requiring the Production of Tangible Things* [etc.], Dkt. No. BR 13-80 (F.I.S.C. Apr. 25, 2013), made it clear that the mass acquisition of Americans' call details extends beyond customers of Verizon, encompassing all wireless and landline subscribers of at least the country's three largest phone companies. *See* Siobhan Gorman et al., *U.S. Collects Vast Data Trove,* Wall St. J., June 7, 2013, http://on.wsj.com/11uD0ue ("The arrangement with Verizon, AT&T and Sprint, the country's three largest phone companies means, that every time the majority of Americans makes a call, NSA gets a record of the location, the number called, the time of the call and the length of the conversation, according to people familiar with the matter.").

[2] http://ktla.com/2015/06/03/president-obama-signs-usa-freedom-act-limiting-nsas-access-to-americans-phone-records/

Additionally, in light of the Second Circuit's recent ruling in *ACLU v. Clapper*, 2015 U.S. App. LEXIS 7531 *4 (2d Cir. May 7, 2015), in which that court held that the metadata collection was beyond the scope of Section 215, now is an appropriate time for this Court to revisit the same issue, but with the benefit of adversarial legal presentation. Particularly relevant to this Court's consideration of allowing Movants' to argue in opposition to Respondents' filed, or soon-to-be filed, petition to recommence metadata collection, the Second Circuit conducted a constructive analysis of the benefit provided by adversarial proceedings vis-à-vis *ex parte* proceedings. *Id* at *104-112 (Sack, J., concurring).

Congress itself has expressed its desire to see more adversarial input by its inclusion of the amicus curiae provision in Section 401 of the USA Freedom Act. Under that authority, the presiding judge of this Court may designate counsel herein as amicus curiae. Movant FreedomWorks is amenable to such a designation by this Court, as an alternative to proceeding under this Motion in Opposition. Accordingly, counsel for Movants is experienced in addressing privacy matters, civil liberties issues and is a constitutional lawyer. Additionally, counsel for Movants serves as lead counsel in *Paul v. Obama*, No. 1:14-cv-262-RJL (D. D.C.) and as such is conversant in the specific statutory and constitutional issues that will be the basis of this Motion in Opposition.

ARGUMENT

Having no guidance from the Court at this stage regarding the level of detail and length of argument this Court would prefer in a motion such as this one, Movants present herein an abbreviated argument, with the request that the opportunity for supplementation and oral argument be granted by the Court.

Movants' first argument is that Respondents' metadata collection is beyond the scope of what Congress authorized in Section 215 and this Court should deny Respondents' filed or imminent request to renew/re-institute such metadata collection. *ACLU v. Clapper*, 2015 U.S. App. LEXIS 7531.

Movants' second argument is that Respondents' metadata collection, as well as the storing and searching of such metadata, violates the Fourth Amendment.

Argument 1: Past and Proposed Metadata Collection Exceeds the Scope of Section 215

Movants acknowledge that presumably every judge of this Court has previously found that the metadata collection was authorized under Section 215 and thus may be uncomfortable effectively overruling prior orders of this Court on such a basis. However, the straightforward set of propositions accepted by the Second Circuit in *ACLU v. Clapper* demonstrates that the metadata collection is beyond the scope of Section 215 and this Court should adopt the position of the Second Circuit. Specifically, Section 215 (50 U.S.C. § 1861) requires that the government's application for an order to produce business records or other tangible things include: "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) of this section..." *Id.* § 1861(b)(2)(A) (emphasis added). *ACLU v. Clapper* noted that "something is 'relevant' or not in relation to a particular subject.... In keeping with this usage, § 215 does not permit an investigative demand for any information relevant to fighting the war on terror, or anything relevant to whatever the government might want to know. It permits demands for documents 'relevant to an authorized *investigation*.'" *ACLU v. Clapper*, at *67 (emphasis in original). The Second Circuit went on to state that "the government effectively

argues that there is only one enormous 'anti-terrorism' investigation, and that any records that might ever be of use ... are relevant to the overall counterterrorism effort. The government's approach essentially reads the 'authorized investigation' language out of the statute." *Id* at *68.[3]

Argument 2: Past and Proposed Metadata Collection, Storage and Searching Violates the Fourth Amendment

I. MOVANTS 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 [Movants] which the Fourth Amendment was designed to protect." *Rakas*, 439 U.S. at 140. In the circumstances of this dispute, the facts demonstrate that Movants' privacy expectation in their telephone metadata the Government seized, stored, and searched for five years – and proposes to continue – 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, i.e., no specific investigation. 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

---

[3] 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).

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)).

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). Presaging the metadata collection, Justice Brennan observed,

> 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 (1983) (citations omitted and emphasis added). Those concerns have been brought to fruition by the use of nearly unimaginably

powerful computing technology. Respondents in this case began casting that dragnet over nine years ago to sweep up the telephone metadata from as many phone calls made to, from, or within the United States as they could.

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 Movants' 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.

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.

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.

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).[4]

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 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*.).

CPNI, as defined in the 1996 Act[5], matches up nearly identically with the metadata being seized by Respondents in this case:

---

[4] 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.
[5] 47 U.S.C. § 222(h)(1).

Telephone Metadata[6]	CPNI Equivalent[7]
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

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"[8] 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.

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. **Respondents vehemently protest that the information they are**

---

[6] *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).
[7] 47 U.S.C. § 222(h)(1).
[8] The definition of "confidential phone records information" in 18 U.S.C. § 1039(h)(1) is virtually identical to the definition of CPNI, and similarly includes the phone records collected by Respondents.

seizing does not identify anyone individually; however, Respondents' 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 Section 215 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.

C. The Information Obtained by the Metadata Collection Is Highly Personalized and Sensitive, Particularly in the Aggregate

Contrary to Respondents' numerous public 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, 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)[9] ("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.*

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.*

Indeed, the President's Review Group on Intelligence and Communications Technologies came to the same conclusion about the collected metadata collection 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.[10]

---

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

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

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

1. Movants 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, Movants 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 information 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), *aff'd sub nom, Riley v. California*, 134 S. Ct. 2473 (U.S. 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.[11]

Treating contractual protections with the dignity of property rights is supported by the majority opinion in *Katz*. "[W]hat a person ***knowingly exposes to the public***, even in his own

---

[11] *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).

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 Movants 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 Respondents seize that metadata, even if such metadata is obtained from Movants' telephone service providers. As best Movants can discern, such bases for Fourth Amendment protection have not previously been briefed for this Court.

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 steps to exclude the outside world—the "public"—from accessing that information.[12] 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

---

[12] 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.

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.[13]

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 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.

2. Movants' 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 Movants' 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

[13] 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).

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 matter at hand, 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);[14] and *Katz*, 389 U.S. 347 (Fourth Amendment protects contents of telephone conversation made within phone booth).[15]

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, Movants have contractual permission to use the telephone system.

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

3. Movants 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.

---

[14] *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).

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

4. Movants 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.[16]

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

The foregoing comparisons lead to the same conclusion as in *1960 Jones*—Movants' 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, Movants 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, Movants reasonably expected their sensitive metadata would neither be broadcast to the world nor handed over to the Government.

---

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

"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. Movants 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. Movants' contracts to preserve the privacy of their telephone metadata constitute objectively observable evidence of Movants' 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. *Smith v. Maryland* Is Inapplicable to this Motion In Opposition

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

Respondents overwhelmingly rely on *Smith v. Maryland*, 442 U.S. 735 (1979), in their arguments in support of their metadata collection. That reliance is misplaced. The differences between present circumstances and *Smith* in 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. 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 matter before this Court, 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, i.e., his phone was an instrument in the commission of a criminal offense. However, in the current circumstances there is no known or suspected crime at the time of metadata collection, and certainly none associated with any particular phone or its usage. Furthermore, there is no known or suspected crime at the time of Respondents' searches of the metadata, at least not associated with Movants' metadata nor the vast number of other individuals' data in Respondents' database.

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 has been seized, stored, kept, and searched for five years with no relation of Movants' data to any case whatsoever, and Respondents propose to continue such violations for 180 more days under Section 215.

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 Movants' 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 nine 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.

h. In *Smith*, nothing but the date, time, and phone numbers involved in a phone call were captured, whereas with the metadata collection, 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).

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%)[17] as households had landlines in 1979 (approx. 91%).[18]

j. At the time of *Smith*, Americans had no choices among phone companies. There was only AT&T with a resulting lack of competition in the terms offered to subscribers. Thus, while Movants today are protected by *contractual privacy* terms, that was not the case for Mr. Smith. Similarly, Respondent Smith did not benefit from the *statutory* privacy protections implemented after *Smith* was decided.

Given the differences in circumstances between *Smith* and this case, the Court should find *Smith* inapplicable and deny Respondents' Motion to Re-institute Metadata Collection.

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

In Respondents' briefs in a variety of cases, they take the position that the so-called "third-party disclosure doctrine" purportedly derived from *Smith v. Maryland* and *United States v. Miller*, 425 U.S. 435 (1976), 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

---

[17] 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.

[18] 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).

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).

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); *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).

Fourth, federal courts have 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[19] 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 Circumstances

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,

---

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

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 physical 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[20] 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).

---

[20] 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).

The concurrences noted that "physical intrusion is now unnecessary to many forms of surveillance." *Id.* at 955 (Sotomayor, J., concurring),[21] 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 Movants 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 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

---

[21] 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).

dialed. In the current circumstances, millions of individuals Respondents acknowledge to be innocent of suspicion for *anything* have been surveilled for nearly 3,300 days as of the filing of this motion. The means used – and proposed to be continued in use – for Respondents' surveillance of Movants and others 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 Respondents' Motion seeking to re-institute/renew the metadata collection should be denied, and other appropriate relief should be granted. [22]

II. MOVANTS' METADATA HAS BEEN BOTH SEIZED AND UNREASONABLY SEARCHED BY RESPONDENTS UNDER THE METADATA COLLECTION

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

---

[22] If the Court finds *Smith* dispositive of Movants' claims, *Smith*'s holding should be revisited. 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). Movants raise this argument solely to preserve a challenge to *Smith*'s holding in the event a court finds *Smith* requires the dismissal of Movants' claims.

A. Respondents' Interference with Movants' Possessory Interest in Their Metadata Constitutes a Seizure Because It Eliminates Movants' Contractual Possessory Rights in Their Metadata

As previously discussed, Movants 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).

In the circumstances before this Court, Movants' contracts with the telephone companies preserve their right to exclude others from viewing their metadata. The metadata collection does not merely *interfere* with Movants' possessory right to exclude others from viewing their metadata. It completely *eliminates* that right.

Furthermore, it is constitutionally unacceptable for the Government to make a copy[23] of a full set of data that includes data the Government had no probable cause to seize and then to

---

[23] 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

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"). Contrary to the Government's likely assertion that "container" cases control, computer data 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.

B. The Metadata Collection Constitutes an Ongoing Unreasonable Search of Movants' Metadata

The Fourth Amendment prohibits "unreasonable searches and seizures." 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 Metadata Collection 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"

---

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).

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 – or proposing to violate – Movants' 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.

The Government often argues – as it did in *ACLU v. Clapper* – 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.[24] 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, Movants have an expectation of privacy in their metadata and American society recognizes that expectation as reasonable. Therefore, the metadata collection constitutes a "search" for purposes of the Fourth Amendment.

2. The Metadata Collection 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)).

The Government may argue 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 government interest justifying blanket suspicionless

---

[24] 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.

searches of the entire American population as a way to *develop* evidence, rather than as a *response* to evidence.[25] In other words, the ends justify the means.

The Government has also nakedly contended the metadata collection is justifiable because it is a *faster way* to develop evidence than other methods. 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 metadata collection 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). 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.[26] "Even where the government claims 'special needs,' a warrantless search *is generally unreasonable* unless based on 'some quantum of individualized suspicion.'" *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).

---

[25] Movants strongly believe fighting terrorism is a critical role of government.

[26] *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).

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).

Movants have established the reasonableness of their significant interest in maintaining the privacy of their telephone metadata, and it is clear the metadata collection intrudes upon that interest. The remaining factors—the nature and immediacy of the Government's concerns and the efficacy of the metadata collection in meeting them—tips strongly in favor of Movants.

First, while Movants do not dispute the importance of identifying terrorist operatives and preventing terrorist attacks, such an interest does not justify a secret blanket warrantless search 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 roadblock set up to thwart* ***an imminent terrorist attack***." 531 U.S. at 44 (emphasis supplied).[27] The word "imminent" is critical. Its primary definition is "[o]f an event, esp. danger or disaster:

[27] 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.

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 a general concern that "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 metadata collection because it is not based on thwarting an "imminent" attack. *Cf. 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.").

Second, the Government has been unable to cite to a single example of the metadata collection 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."[28] Notably,

---

[28] Brief of *Amici Curiae* Senators Ron Wyden, Mark Udall, and Martin Heinrich in Support of Movants, *First Unitarian Church of L.A. v. Nat'l Security Agency*, No. 3:13-cv-03287-JSW, at 2 (N.D. Cal.),

the senators contend the Government's claim the metadata collection has helped "thwart" or "disrupt" 54 specific terrorist plots **is untrue** because the metadata collection 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."[29] 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.[30]

Third, when the Government asked the FISC to authorize the metadata collection, 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 intelligence activities,[31] 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).[32] 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.[33]

Docket Entry 63-2 (filed Nov. 18, 2013) (hereinafter "Senators' Brief"). Mark Udall lost his re-election in 2014 and is no longer a Senator.

[29] *Id.* at 6–7.

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

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

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

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

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 metadata collection 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).[34] Thus, the FISC's suspicions in March 2009 were well-founded, as the Government no longer characterizes the metadata collection as indispensable. Moreover, if the Government itself concedes the program is not "vital," it seriously undercuts the "special needs" argument.

Finally, even if the metadata collection 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.[35] "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

---

[34] 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 become public.

[35] *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).

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 metadata collection violates the Fourth Amendment because it constitutes an impermissible seizure and an unreasonable search.

III. 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 *Kyllo*, 533 U.S. at 34); *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).

In 1792, the primary means of communication was by mail instead of phone,[36] 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*

---

[36] 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*).

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.[37] 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.

Furthermore, 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,[38] and presumably a similar number by 1792. 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.[39] Crime victims presented their own cases to courts until the late 19th century.[40]

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 metadata collection. 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 herein, this Court should

---

[37] Available at https://www.rutherford.org/files_images/general/2014_Historic_4th_Amendment-NSA_Metadata.pdf (as of May 14, 2014).
[38] *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).
[39] Walker, S., *Popular Justice: A History of American Criminal Justice* at 25 & 29 (2d ed. 1998).
[40] *Id.* at 71.

also find that the metadata collection falls not only below the level of privacy an American would have expected in 1792, but that it does so today as well.

CONCLUSION AND PRAYER FOR RELIEF

For all the foregoing reasons, the Court should deny the Government's request to re-institute/renew metadata collection. Furthermore, the Court should declare that the metadata collection is beyond the scope of Section 215 and violated the Fourth Amendment; enjoin Respondents from conducting or operating the metadata collection; order Respondents to destroy any and all telephone metadata that has been seized, stored, retained, and/or searched, regardless where held or by whom (excepting such data as Respondents can show reasonable cause to be related to an authorized investigation); award Movants' fees and costs pursuant to 28 U.S.C. 2412; and such other and further relief as the Court deems just and proper.

Respectfully Submitted,

Kenneth T. "Ken" Cuccinelli, II
KCuccinelli@CuccinelliAndAssociates.com
Cuccinelli & Associates, PLLC
13881 Jordan Meadows Lane
Nokesville, Virginia 20181
Ph: (804) 286-2550
No fax number
Counsel for Movants

Certificate of Service

I certify that a true and correct signed electronic original, as allowed under Rule 7 of this Court, of the foregoing Movants' Motion In Opposition to Government's Imminent or Recently-Made Request To Resume Bulk Data Collection Under Patriot Act § 215 was filed with the Court and served on all of the following by e-mail sent to Joan Kennedy, Associate Director, Security and Emergency Planning Staff, Litigation Security Group, United States Department of Justice, as prearranged in accordance with Rule 8 of this Court on June 4, 2015:

Barack H. Obama
Office of the President, The White House
1600 Pennsylvania Ave., N.W.
Washington, DC 20500

James R. Clapper
Director of National Intelligence;
Office of the Director of National Intelligence
Attn: James R. Clapper
Washington, D.C. 20511

Adm. Michael Rogers
Director of the National Security Agency and Chief of the Central Security Service
National Security Agency
9800 Savage Rd.
Fort Meade, MD 20755

James B. Comey, Jr.
Director of the Federal Bureau of Investigation
FBI Headquarters
935 Pennsylvania Avenue, N.W.,
Washington, D.C. 20535-0001

Ken C II

Kenneth T. Cuccinelli, II