[ORAL ARGUMENT SCHEDULED FOR NOVEMBER 4, 2014]

Nos. 14-5004, 14-5005, 14-5016, 14-5017

IN THE

UNITED STATES COURT OF APPEALS

FOR THE

DISTRICT OF COLUMBIA CIRCUIT

LARRY ELLIOT KLAYMAN ET AL.,
Plaintiffs—Appellees / Cross-Appellants,

— v. —

BARACK HUSSEIN OBAMA ET AL.
Defendants—Appellants / Cross-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

REPLY BRIEF OF PLAINTIFFS—APPELLEES / CROSS-APPELLANTS

LARRY KLAYMAN
Attorney at Law
D.C. Bar No. 334581
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006
Phone: (310) 595-0800
Email: leklayman@gmail.com

October 3, 2014

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

GLOSSARY

"ACLU" refers to the American Civil Liberties Union

"Felten Aff'd." refers to Expert Felten's Affidavit

"Felten Supp. Aff'd." refers to the Supplement to Expert Felten's Affidavit

"DOJ" refers to the Department of Justice

"FISA" refers to the Foreign Intelligence Surveillance Act of 1978

"FISC" refers to the United States Foreign Intelligence Surveillance Court

"FTC" refers to the Federal Trade Commission

"Gov't Reply Brief " refers to the Government Defendants' Response and Reply Brief

"NSA" refers to the National Security Agency

"CNSS" refers to the Center for National Security Studies

"SA" refers to the Supplemental Appendix

"Section 215" refers to Section 215 of the Patriot Act, Public Law 107–56—Oct. 26, 2001

"VBSN" refers to Verizon Business Network Services

"***When governments fear the people, there is liberty. When the people fear the government, there is tyranny.***"

- Founding Father and President Thomas Jefferson

"***[T]he Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself.***"

- Supreme Court Chief Justice John Roberts in *Riley* v. *California*, 134 S.Ct. 2473, 2494 (2014)

"***This is a case at the pinnacle of public national interest.***"

- The Honorable Richard J. Leon in *Klayman v. Obama* at the Status Conference of October 31, 2013

SUMMARY OF ARGUMENT

Plaintiffs—Appellees/Cross-Appellants ("Plaintiffs") hereby reply to Defendants—Appellants/Cross-Appellees' ("Government Defendants") Response and Reply Brief ("Response and Reply Brief").

The Government Defendants, in their Response and Reply Brief, completely sidestep the crucial constitutional issues regarding the First and Fifth Amendments. This Court must decide these issues involving the First and Fifth Amendments because they are just as important as Plaintiffs' Fourth Amendment claim, in which the United States District Court for the District of Columbia ("District Court") found that

Plaintiffs had standing to bring. The significance of metadata in addition to the district court's ruling in the present case establishes standing to challenge the Section 215 illegal government surveillance of bulk telephony metadata. Further, the Government Defendants distort the significance of the Supreme Court's groundbreaking decision in *Riley* v. *California*, 134 S.Ct. 2473 (2014), as *Riley* is controlling and *Smith v. Maryland*, 442 U.S. 735 (1979) is inapplicable under the circumstances in the present case. Finally, the government defendants cannot establish a "special need" to warrant the use of the Section 215 illegal government surveillance of bulk telephony metadata.

Accordingly, this Court must respectfully affirm the District Court's Order of December 16, 2013, preliminarily enjoining the Government Defendants from continuing to illegally and unconstitutionally conduct surveillance on Plaintiffs, and hundreds of millions of Americans. The NSA has been unlawfully accessing telephony metadata of not only Plaintiffs, but hundreds of millions of Americans, that clearly exceeds Constitutional protections. The Government Defendants' illegal surveillance of Plaintiffs' and virtually all 300 million Americans has had, and will continue to have, a

prominent chilling effect on the right to feel and be secure in one's own home. This is the very thing that harms the American people because such a chilling effect inhibits their speech due to the reasonable fear that the government will continue to spy on their most intimate moments.

In making a decision, this Court must thus consider the national importance of this case as it is also believed by many to be the most important case to come before this Court. Plaintiffs merely want to preserve the status quo by simply having the Government Defendants obey the law, which will ultimately not harm anyone.

STATUTES AND REGULATIONS

All applicable statutes and regulations are contained in Appellees/Cross-Appellants' opening brief.

ARGUMENT

I. THE GOVERNMENT DEFENDANTS' RESPONSE AND REPLY BRIEF SIDESTEPS THE CRUCIAL CONSTITUTIONAL ISSUES REGARDING THE FIRST AND FIFTH AMENDMENTS.

The Government Defendants merely rehash the same arguments that were rejected by the District Court and circumvent the reality that Plaintiffs' First and Fifth Amendment claims, which have not been

ruled upon, are just as important as Plaintiffs' Fourth Amendment claim. As the District Court ultimately found that Plaintiffs have made a sufficient showing to merit injunctive relief on their Fourth Amendment claim, Supplemental Appendix ("SA") 5 n.7, the District Court decided to not reach their other constitutional claims under the First and Fifth Amendments, and thus this Court should reach a decision regarding these additional Amendments as well.

The Supreme Court has frequently emphasized the importance of preserving the First Amendment rights of advocacy groups, recognizing that the government's surveillance and investigatory activities infringe on associational rights protected by the amendment. In *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958), the Supreme Court invalidated an Alabama order that would have required the NAACP to disclose its membership list. The Supreme Court wrote, in explaining why the protection of privacy is of particular Constitutional concern for advocacy organizations:

> "[I]t is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute an effective restraint on freedom of association as the forms of governmental actions . . . were thought likely to produce upon the particular constitutional rights there involved. This Court has recognized the vital relationship between freedom to

> associate and privacy in one's association . . . inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." *Alabama*, 357 U.S. at 462.

As discussed above, the Government Defendants' broad sweeping surveillance program raises precisely the same harm. In light of his public advocacy in matters of public interest and concern, Plaintiff Klayman, an attorney, regularly communicates with individuals who wish to come forward with evidence of government wrongdoing, such as depriving them of their civil rights. Likewise, Plaintiff Klayman also regularly engages in telephone calls with potential clients and clients he is already representing, wherein he discusses legal matters and advises the clients, whistleblowers, and others regarding legal strategies and techniques. Similarly, Plaintiffs Charles and Mary Ann Strange, who are activists in advocating change in U.S. military policies and practices, routinely communicate, via phone to clients, potential clients, supporters, and others, regarding the advocacy plans, tactics, strategies and goals. Given the nature of their advocacy, and the inherent effects on government policy and acts, Plaintiffs' communication records

contain confidential and legally-privileged discussions that must not be collected, monitored, heard, or recorded by the government.

Plaintiffs enjoy a liberty interest in their personal security and in being free from the Government Defendants' use of unnecessary and excessive force or intrusion against his person. Plaintiffs also enjoy a liberty of not being deprived of life without due process of law.

In *ACLU v. Clapper,* 959 F. Supp. 2d 724 (2014), a substantially related case, the ACLU addressed in its appellate brief before the United States Court of Appeals for the Second Circuit ("Second Circuit") the governments' First amendment violations by arguing that the "district court erred in holding that the [illegal government surveillance] does not cause any cognizable injury to Plaintiffs' First Amendment rights." "Safeguards required by the Fourth Amendment may in some contexts satisfy the First Amendment as well—for example, a criminal search warrant may satisfy both the First and Fourth Amendments if it is carefully drawn and supported by probable cause." *See, e.g.*, *Zurcher v. Stanford Daily*, 436 U.S. 547, 565 (1978); *United States v. Ramsey*, 431 U.S. 606, 623–24 (1977).

The chilling effect on Plaintiffs' contacts also effects a substantial impairment of Plaintiffs' First Amendment rights. The ACLU cited to *Shelton v. Tucker*, 364 U.S. 479 (1960), an instructive Supreme Court case. "In that case, the Court found that First Amendment rights were substantially burdened by an Arkansas law requiring teachers to 'disclose every single organization with which [they had] been associated over a five-year period.' *Id.* at 487–88." In *Shelton*, the Supreme Court "adopted a commonsense approach and recognized that a chilling effect was inevitable if teachers who served at the absolute will of school boards had to disclose to the government all organizations to which they belonged." *Local 1814, Int'l Longshoremen's Ass'n, AFL–CIO v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 272 (2d Cir. 1981). The chilling effect is equally inevitable in *ACLU v. Clapper*, as well as in the present case. Plaintiffs suffer a further injury because of the illegal government surveillance's chilling effect on their contacts and sources.

For the stated reasons, this Court should nonetheless reach a decision pertaining to these Constitutional claims.

II. PLAINTIFFS HAVE STANDING TO CHALLENGE THE SECTION 215 ILLEGAL GOVERNMENT SURVEILLANCE OF BULK TELEPHONY METADATA.

A. The Government Defendants Distort The Significance Of The Supreme Court's Groundbreaking Decision In *Riley*, As *Riley* Is Controlling And *Smith* Is Inapplicable Under The Circumstances In The Present Case.

The Supreme Court's recent landmark decision in *Riley* invalidates the Supreme Courts' previous ruling in *Smith* **in the context of this case**. In realizing the prominent effect that *Riley* has in this case, the Government Defendants try to argue that "the force and controlling precedential effect of *Smith* has not been altered by changes in technology or the Supreme Court's decision in *Riley*[ ]," Gov't Reply Brief at 3, as an attempt to downplay the significance of *Riley*. The Government Defendants also argue that "Plaintiffs fundamentally misunderstand the basis and scope of *Riley*." Gov't Reply Brief at 18. The Government, however, is overwhelming misguided. In fact, "the Supreme Court [ ] distance[d] itself from *Smith* when it ruled unanimously [ ] against cellphone searches in *Riley v. California*. Nicandro Lannacci, *NSA surveillance moves one step closer to the Supreme Court*, Constitution Daily (Sept. 5, 2014), available at

http://blog.constitutioncenter.org/2014/09/nsa-surveillance-moves-one-step-closer-to-the-supreme-court/.

In *Riley*, Chief Justice John Roberts spoke, and acknowledged the importance and advancement of today's phone technologies and metadata. *See Riley*, 134 S.Ct. at 2489 (explaining that cell phones today could "just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers"). This Court must follow *Riley* as it is the new law of the land.

Chief Justice John Roberts held that police generally must obtain a warrant before searching a cell phone seized incident to an arrest due to the amount of personal and sensitive information that can now be found on any person's cellphone. *See Riley*, 134 S.Ct. at 2489-93. The Supreme Court found that "[M]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life[.]" *Id.* at 2494. The Supreme Court also recognized that "more substantial privacy interests are at stake when digital data is involved" because "cell phones can store millions of pages of text, thousands of pictures, or

hundreds of videos. . . . [which] [have] several interrelated privacy consequences." *Id.* at 2478. Chief Justice John Roberts, in delivering the majority opinion, even found that "modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Id.* at 2484.

The Supreme Court's modern up-to-date view of today's cellular phones has surely impacted the extent that the Government Defendants can lawfully intrude upon citizens' rights. In fact, *Riley* in the context of this case, eliminates *Smith*. This is not a pen register, this is metadata, and with it, the Government invades and accesses every aspect of our lives, far beyond even that which is contained on a smart cell phone.

In further discussing the relevance of cellular data when it is unlawfully searched by the Government, the Supreme Court held that "a search of digital information on a cell phone does not further [ ] government interests . . . and implicates substantially greater individual privacy interests than a brief physical search." *Id.* at 2478. Due to the highly sensitive data located in our cell phones, the Supreme

Court made it clear that a warrant is generally required before a search, even when a cell phone is seized incident to arrest. *Id.* at 2495. Because "[d]igital data stored on a cell phone cannot itself be used as a weapon" and "can endanger no one," the Government Defendants do not have a compelling reason to search citizens' telephony and internet metadata at their discretion. *See id.* at 2485.

Furthermore, unlike in *Riley*, the NSA has access to, and did access, entire telephone conversations, which it keeps stored for at least five years in the Government Defendants' super computers. Although these reasons alone are enough to find that the Government Defendants violated Plaintiffs' rights, and that they should be prevented from further violating them, there is much more this Court can consider.

The Supreme Court, in the outdated *Smith* decision, could not have predicted the extent that cellular technology would advance, nor could it have predicted the extent that data would be searched, the Supreme Court found that today's technology was nearly inconceivable just a few decades ago. *Riley*, 134 S.Ct. at 2484 ("Even less sophisticated phones [,such as a flip phone] . . . , which have already faded in popularity since Wurie was arrested in 2007, have been around

for less than 15 years. Both phones are based on technology nearly inconceivable just a few decades ago,[1] when *Chimel*[2] and *Robinson*[3] were decided [in 1969 and 1973, respectively]"). Justice Samuel Alito, who concurred in part and dissented in part, "agree[d] that we should not mechanically apply the rule used in the predigital era to the search of a cell phone." *Riley*, 134 S.Ct. at 2496. The Supreme Court's ruling in *Riley* clearly lays the foundation for what is to come in the present case—that is, that past Supreme Court rulings, around the time of *Smith*, analyzing unlawful police and government searches, do not apply to the then unforeseeable circumstances of today. *Smith* was issued by the Supreme Court over thirty-five (35) years ago!

Although "[t]he analysis of this threshold issue of the expectation of privacy must start with the Supreme Court's [ ] opinion in *Smith* . . . ," the District Court properly determined that *Smith* is not applicable as

---

[1] "Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Riley*, 134 S.Ct. at 2489.

[2] In *Chimel v. California*, 695 U.S. 752, 753-54 (1969), the Police searched just one home. In the present case, the Government Defendants are searching the pockets of over 300 million citizens. The amount of information found in one's cell phone is more than the amount of information found in one's home.

[3] *United States v. Robinson*, 414 U.S. 218 (1973).

the Supreme Court justices in 1979 could not have envisioned the full extent that, or how, technology would advance. SA 49.[4]

In *Smith,* police were investigating a robbery victim's reports that she had received threatening and obscene phone calls from someone claiming to be the robber. *Smith*, 442 U.S at 737. Without obtaining a warrant or court order, police installed a pen register, which revealed that a telephone in Smith's home had been used to call the victim on one occasion. *Id.* The Supreme Court held that Smith had no reasonable expectation of privacy in the numbers dialed from his phone because he voluntarily transmitted them to his phone company, and because it is generally known that phone companies keep such information in their business records. *Id.* at 742-44.

The District Court properly disagreed with the Government Defendants' main argument, that under *Smith*, no individual has an expectation of privacy, or even a reasonable one, in any and all collected telephony metadata, and thus, the illegal government surveillance of bulk telephony metadata is not a search. Govt.'s Opp'n at 45–50. In

[4] "[T]he almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979 . . . ." SA 49.

making this determination, the District Court ruled that the question before the District Court was "*not* the same question that the Supreme Court confronted in *Smith* [and,] [t]o say the least, 'whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment,' . . . —under the circumstances addressed and contemplated in that case—is a far cry from the issue in this case."

The question in the present case asks, "[w]hen do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply?" SA 47. The District Court simply answered, "now." *Id.* Consequently, the District Court ruled that the bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.

In comparing the circumstances in *Smith* to the circumstances in this case, the District Court noted that pen register in *Smith* was operational for only a matter of days, and with no indication the

Government would retain any of the limited phone records once the case was over. *See* 442 U.S. at 737. A key difference in *Smith* is that "the short-term, forward-looking (as opposed to historical), and highly-limited data collection is [ultimately] what the Supreme Court was assessing." "The NSA['s illegal government surveillance of] telephony metadata [ ], on the other hand, involves the creation and maintenance of a historical database containing [at least] *five years* ' worth of data." Moreover, the relationship between the police and the phone company in *Smith* is incomparable to the relationship that has evolved over the last seven years between the Government Defendants and all of the telecom companies. In *Smith,* the Supreme Court considered a one-time, targeted request for data regarding an individual suspect in a criminal investigation, whereas the Court here must consider the NSA's "daily, all-encompassing, indiscriminate dump of phone metadata that the NSA now receives as part of its [illegal government surveillance of] [b]ulk [t]elephony [m]etadata [ ]." SA 48.

The District Court further explained why *Smith* does not apply in the present case by pointing out that "not only is the Government's ability to collect, store, and analyze phone data greater now than it was

in 1979, but the nature and quantity of the information contained in people's telephony metadata is much greater, as well." SA 50. Cell phones did not exist in 1979; today, they are used for many purposes other than calling, and thus people now have an entirely different relationship with phones than they did in 1979.[5] SA 54. Metadata today, the District Court stated, "reflects a wealth of detail about . . . familial, political, professional, religious, and sexual associations," and "reveal[s] an entire mosaic—a vibrant and constantly updating picture of the person's life." *Id.*

"In sum, [the District Court ruled that] the *Smith* pen register and the ongoing NSA [illegal government surveillance of] [b]ulk [t]elephony [m]etadata [ ] have so many significant distinctions between them that [the District Court] cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones." SA 55. "[T]rends have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable." *Id.* at 54. In analyzing whether Plaintiffs

[5] "According to the 1979 U.S. Census, in that year, 71,958,000 homes had telephones available, while 6,614,000 did not. U.S. Dep't Of Commerce & U.S. Dep't Of Hous. & Urban Dev., Annual Housing Survey: 1979, at 4 (1981).

have a reasonable expectation of privacy that is violated when the Government Defendants collected and searched their telephony metadata, the District Court determined that it was significantly likely it would answer in Plaintiffs' favor. SA 56. The District Court found that the "[P]rogram infringes on '[the] degree of privacy' that the Founders enshrined in the Fourth Amendment," and subsequently "grant[ed] [Plaintiffs'] requests for a[ ] [preliminary] injunction[.]" SA 64.

As such, the outdated ruling in *Smith* does not foreclose Plaintiffs arguments.

B. The Significance Of Metadata As Held By The District Court's Ruling In The Present Case Establishes Standing To Challenge The Section 215 Illegal Government Surveillance Of Bulk Telephony Metadata.

The Government Defendants ultimately hold the cards and they refuse to reveal their hand in fear that Plaintiffs' and the District Courts' conclusions are accurate. Regardless, discovery is not needed due to the highly intrusive nature of metadata, which is well-known and established as an uncontroverted fact, as explained by Expert Edward W. Felten ("Expert Felten") and as previously determined by the District Court.

Expert Felten, a professor of computer science and public affairs, as well as Director of the Center for Information Technology Policy at Princeton University, who also served as the first Chief Technologist at the U.S. Federal Trade Commission (FTC), explains the highly sensitive and intrusive nature of metadata. *See* Felten Aff'd. at 1-3. Expert Felten begins by explaining that many details of our lives can be gleaned by examining metadata, which often yields information more easily than do the actual content of our communications. *Id.* at 1. "Telephony metadata is easy to aggregate and analyze." *Id.* at 7. For instance, metadata "naturally reveals information about the location of the parties." *Id.* at 6,[6] and "as a result, individual pieces of data that previously carried less potential to expose private information may now, in the aggregate, reveal sensitive details about our everyday lives—details that we had no intent or expectation of sharing." *Id.* at 8. It is practically impossible for individuals to avoid leaving a metadata trail when engaging in real-time communications, such as telephone calls or

[6] "For example, even if the government never obtains cell site location information about a call, trunk identifier information revealing that a domestic call was carried by a cable from Hawaii to the mainland United States will reveal that the caller was in the state of Hawaii at the time the call was placed." *Id.* at 6-7.

Internet voice chats. *Id.* at 11. Even when people try to prevent the government from accessing their metadata and private information, "secure communication technologies protect only the content of the conversation and do not protect the metadata." *Id.* at 12. In fact, there is no practical way to prevent the creation of telephony metadata, or to erase it after the fact. The only reliable way to avoid creating such metadata is to avoid telephonic communication altogether. *Id.* at 13. Expert Felten then points out that:

> "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. As such, a universal database containing records about all Americans' communications will reveal vastly more information, including new observable facts not currently known to the research community, because no researcher has access to the kind of dataset that the government is presumed to have." *Id.* at 21-22.

Another reason why metadata is so important to each individual is because, like social security numbers or individual taxpayer identification numbers, phone numbers are unique to their owners. Felten Supp. Aff'd. at 2.

In further understanding the importance of metadata, as Expert Felten explained in his affidavits, the District Court found it Orwellian that the Government Defendants had in fact searched Plaintiffs' and all other citizens' metadata without proper judicial approval. *See* SA 56.

Also, in determining whether Plaintiffs met the requirements for standing, the District Court analyzed *Clapper v. Amnesty International USA*, 133 S.Ct. 1138 (2013) and ultimately ruled that the facts that arise in Plaintiffs' claims are distinguishable from *Clapper*.[7] In *Clapper*, where the plaintiffs "could only speculate as to whether they would be surveilled at all, [P]laintiffs in [*Klayman I*][8] can point to strong evidence that, as Verizon customers, their telephony metadata has been collected for the last seven years (and stored for the last five) and will continue to

[7] "In *Clapper*, the Supreme Court held that the plaintiffs lacked standing to challenge NSA surveillance under FISA because their 'highly speculative fear' that they would be targeted by surveillance relied on a 'speculative chain of possibilities' insufficient to demonstrate a 'certainly impending' injury. 133 S.Ct. at 1147–50. Moreover, the *Clapper* plaintiffs' 'self-inflicted injuries' (i.e., the costs and burdens of avoiding the feared surveillance) could not be traced to any provable government activity. *Id.* at 1150–53" That is not the case here. SA 26.

[8] Plaintiffs also cross-appeal the ruling in *Klayman II*, where the District Court erred in denying Plaintiffs' request for a preliminary injunction, and in also not including Mary Ann Strange as a Plaintiff since she had been plead as a Verizon subscriber. *See Klayman II* Complaint ¶18 ("Plaintiffs Charles and Mary Ann Strange are consumers, subscribers, and users of Verizon . . . .").

be collected barring judicial or legislative intervention." SA 36-37. The District Court then properly concluded that "[P]laintiffs meet the standing requirements set forth in *Clapper*, as they can demonstrate that the NSA has collected and analyzed their telephony metadata and will continue to operate the illegal government surveillance consistent with FISC opinions and orders." SA 42.

Importantly, however, that the Government Defendants have not denied collecting information about Plaintiffs' calls. Plaintiffs have no need to speculate, and have not speculated, that their metadata has been collected because Plaintiffs have other sufficient evidence, as determined by the District Court, for them to be *certain* their data has been collected for the last seven years based off of the Government Defendants querying procedures. As stated by the District Court, additional support includes the revelation that the Government Defendants have declassified and authenticated a FISC Order signed by Judge Vinson confirming that the NSA has indeed collected telephony metadata from Verizon. Even more compelling, the District Court found that the Government Defendants themselves described the advantages of bulk collection in such a way to convince the Court that "Plaintiff's

metadata—indeed *everyone's* metadata—is analyzed, manually or automatically . . . ." SA 39.

The Government Defendants have acknowledged that, for several months in 2013, they collected business records containing telephony metadata from Verizon Business Network Services ("VBNS"), which, they allege "is not the same entity as Verizon Wireless" and [t]he only support plaintiffs provide for that assumption is their assertion that they are subscribers of Verizon Wireless cellular phone service. App. 98, 101. However, the District Court found that the Government Defendants "must under the Section 215 [illegal government surveillance] collect metadata from all of the three "largest carriers" in order for that [illegal government surveillance] to 'serve its . . . function.'" The District Court was not persuaded by the Government Defendants' argument and ultimately determined that the Government Defendants were "straining mightily" to find a reason that Plaintiffs lack standing to challenge the metadata collection.

The District Court found, however, that "[t]he Government [Defendants] obviously wanted [the District Court] to infer that the NSA may not have collected records from Verizon Wireless (or perhaps

any other non-VBNS entity, such as AT&T and Sprint) [and] [that] the Government [Defendants] [made] this argument at the same time [they are] describing in [their] pleadings an [illegal government surveillance of] bulk metadata . . . that can function *only* because it 'creates a historical repository that permits retrospective analysis of terrorist-related communications *across multiple telecommunications networks,* and that can be immediately accessed as new terrorist-associated telephone identifiers come to light.'" SA 27. Accordingly, the District Court ruled "the NSA . . . collected metadata from Verizon Wireless." SA 27.

Plaintiffs themselves have already shown that they have standing to challenge the illegal government surveillance because Plaintiffs are subscribers of Verizon Wireless cellular telephone services, and their metadata was collected as a part of the Government Defendants' illegal and unconstitutional surveillance.

In addition to the District Court, other courts have found standing in favor of plaintiffs who challenged the Government's illegal government surveillance. For instance, the issue of standing involving almost identical circumstances, and against many of the same

Government Defendants, can be found in *ACLU v. Clapper*, a related case filed in the U.S. District Court for the Southern District of New York ("New York District Court"). The New York District Court found that the plaintiffs also had standing to challenge the Government Defendants' illegal government surveillance because the Government Defendants had collected telephony metadata related to the plaintiffs' telephone calls. The Government Defendants were found to have reviewed the ACLU plaintiffs' records. Similar to Plaintiffs in the present case, every time the NSA queried the phone-records database, it reviewed the ACLU plaintiffs' records to determine whether the plaintiffs or their contacts were connected to a phone number that the NSA deemed suspicious. As such, like the ACLU plaintiffs and the New York District Court, Plaintiffs here and the District Court in this jurisdiction are aware that Plaintiffs' telephony metadata has been searched.

Finally, the Government Defendants' still attempt to argue that the Section 215 illegal government surveillance was discontinued, and thus Plaintiffs' claims are moot. The Government Defendants cannot be trusted—the Section 215 illegal government surveillance was not

discontinued. Even in the event that the Section 215 surveillance was discontinued, which it most certainly was not, Plaintiffs are entitled to damages since the Government Defendants' unlawful violations fell within the statute of limitations in addition to Plaintiffs' request for injunctive relief.

In the recent *ACLU v. Clapper* oral argument[9] held on September 2, 2014, the Second Circuit[10] expressed agreement with the District Court's ruling. Judge Robert Sack of the Second Circuit seemed unconvinced by the government's arguments and said "I wonder about how valid the ratification argument is when you're dealing with secret law." *See* Lannacci, *supra*. He then said, "I thought the ratification notion is you're dealing with something that's public and that by ratifying it again and again you're somehow reflecting the public will because they know about it." *Id.*

Judge Gerard E. Lynch also seemed skeptical of the government's

---

[9] Plaintiffs have attached to the filed hard copies the Audio CD of the American Civil Liberties Union's (ACLU) oral argument against the government before the Second Circuit as Exhibit 1.

[10] The Second Circuit is the first U.S. Appeals Court to consider whether the Section 215 illegal government surveillance is constitutional. Plaintiffs are pleased to have the ACLU and the Center for National Security Studies (CNSS) as *amici*. However, they have both misunderstood Plaintiffs' arguments regarding *Riley v. California*.

arguments. He stated, "'[i]t's hard to imagine that [Section 215's] rather innocuous language' means the government could collect so many records in bulk that have never been acquired before with a grand jury subpoena." Ellen Nakashima, *Federal appeals court hears arguments over NSA's bulk collection of phone records*, Washington Post (Sept. 2, 2014), available at http://www.washingtonpost.com/world/national-security/federal-appeals-court-hears-arguments-over-nsas-bulk-collection-of-phone-records/2014/09/02/cc75ef62-32df-11e4-a723-fa3895a25d02_story.html. He continued, "[y]ou're really saying, 'They're not relevant to an investigation right now; we just want to have them in case they become relevant.'" *Id.* "The panel's three judges, all appointed by Democrats, seemed concerned that the same argument could be extended to other data, such as credit card or bank records." *Id.* Judge Lynch then said to the government, "you can collect everything there is to know about everybody and have it all in one big government cloud. . . . I just don't understand the argument as to what's so special about telephone records that makes them so valuable, so uniquely interactive, that the same arguments you're making don't apply to every record in the hands of a third-party business entity of every American's

everything." *Id.*

"These judges have reason to be skeptical about DOJ's claims about their own surveillance programs. Which is probably why Judge Sack asked 'That's what you've let us know. What else haven't you let us know?'" Empty Wheel, *"What Else Haven't You Let Us Know?" 2nd Circuit Asks DOJ* (Sept. 2, 2014), available at http://www.emptywheel.net/2014/09/02/what-else-havent-you-let-us-know-2nd-circuit-asks-doj/. Like the Honorable Richard J. Leon of the District Court, "the panel seemed particularly concerned that the government's arguments upholding the legality of the telephone metadata program could be applied to other types of data stored with third parties such as banking records and credit card transactions." Elizabeth Banker, *AG, DNI And Judiciary Agree That Congress Should Take Action To Reform Section 215*, ZwillGenblog (Sept. 9, 2014), available at http://blog.zwillgen.com/2014/09/09/ag-dni-judiciary-agree-congress-take-action-reform-section-215/. In fact, "[t]he government tried to distinguish the telephone context from the other financial arena, but the panel seemed somewhat skeptical that the differences were significant and indeed seemed to hold some concern of a 'slippery

slope.'" *Id.* As such, the Second Circuit's concerns demonstrate the relevance of metadata and the consequences that have resulted after the Government Defendants unlawfully searched Plaintiffs' and other citizens' metadata.

For the foregoing reasons, due to the intrusive nature of metadata, as supported by Expert Felten's affidavit and the Second Circuit's concerns, and the absolute fact that Plaintiffs' and all other citizens' metadata has been searched, as the District Court correctly concluded, Plaintiffs have standing to challenge the Section 215 illegal government surveillance.

III. THE GOVERNMENT DEFENDANTS CANNOT ESTABLISH A SPECIAL NEED TO WARRANT THE USE OF THE SECTION 215 ILLEGAL GOVERNMENT SURVEILLANCE OF BULK TELEPHONY METADATA.

The Government Defendants once again argue that if the Section 215 illegal government surveillance could be viewed as effecting a Fourth Amendment search, it would be permissible under the "special needs" doctrine because national security interests outweigh citizens' privacy interests. Gov't Reply Brief at 5. The Government is flawed in their argument once again.

"Even where the government claims 'special needs,'" as it does in this case, "a warrantless search is generally unreasonable unless based on 'some quantum of individualized suspicion.'" SA 57 (quoting *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 624 (1989)). In analyzing the "special needs" doctrine, however, the Honorable Richard J. Leon of the District Court rejected the Government Defendants' argument that the Government Defendants' Fourth Amendment search would nonetheless be permissible, and stated, "To my knowledge . . . no court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion. In effect, the Government urges me to be the first non-FISC judge to sanction such a dragnet." SA 58. Accordingly, the District Court found that "plaintiffs have a very significant expectation of privacy in an aggregated collection of their telephony metadata covering the last five years, and the NSA's Bulk Telephony Metadata Program significantly intrudes on that expectation." *Id.*

Ultimately, there is no reason why the Government needs to search over 300 million Americans' records to allegedly find isolated

occurrences of terrorist activity. Expert Felten himself explained under oath:

> **"**The government states that it could not perform three-hop analysis on a suspect's phone number without first building a database of *everyone's* call records. *See* Gov't PI Opp. 4. This is technologically incorrect. There are a number of ways in which the government could perform three-hop analysis without first building its own database of every American's call records." Felten Aff'd. at 3. "For example, Ms. Shea suggests that the mass call-tracking program would have allowed the government to learn that a 9/11 hijacker (Khalid al- Mihdhar) was in the United States when he communicated with an al Qaeda safe house in Yemen. Shea Decl. ¶ 11. There is absolutely no need for a database of every American's call records to perform this sort of one-hop analysis." *Id.* at 4. "[A] simple connection could [be] discovered directly from the telephone companies without the need for a government database of all call records." *Id.*

Consistent with Expert Felten's affidavit, the District Court properly found that the "Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature. In fact, none of the three 'recent episodes' cited by the Government that supposedly 'illustrate the role that telephony metadata analysis can play in preventing and

protecting against terrorist attack involved any apparent urgency."[11] SA 61.

Accordingly, the District Court ruled that, "[g]iven the limited record before [the District Court] at this point in the litigation—most notably, the utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics—[the District Court] ha[s] serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism. SA 62.

There is no reason to conduct a surveillance of over 300 million Americans when the Government Defendants should be more focused on terrorists themselves, as the Government Defendants have failed to stop one of them. *See id.* In further support, more recently, the Government Defendants were unsuccessful in discovering the rising of ISIS and the force of 50,000 terrorists, even when these terrorists openly communicated with the United States through social media and

[11] The District Court found that "[t]here is no indication that these revelations were immediately useful or that they prevented an impending attack." SA 61.

through other forms of communication. President Obama even criticized the Director of National Intelligence, James Clapper for underestimating the powerful force of ISIS. President Obama stated in a *60 Minutes* interview, "I think our head of the intelligence community, Jim Clapper, has acknowledged that I think they underestimated what had been taking place in Syria." David Jackson, *W. House: Obama not blaming intelligence officials*, USA Today (Sept. 29, 2014), available at http://www.usatoday.com/story/theoval/2014/09/29/obama-islamic-state-josh-earnest-james-clapper-iraq-syria/16433333/. "The United States underestimated the rise of the Islamic State in Iraq and Syria[.] President Obama . . . acknowledged the Iraqi army's inability to successfully tackle the threat." Sebastian Payne, *Obama: United States underestimated rise of Islamic State*, Washington Post (Sept. 28, 2014), available at http://www.washingtonpost.com/blogs/post-politics/wp/2014/09/28/obama-united-states-underestimated-rise-of-islamic-state/.

If our own President claims to have has lost faith in the government's ability to track down terrorists, then there is clearly no justification for the Government Defendants to search all of our

metadata. President Obama even "[a]cknowledg[ed] that the Islamic State has been 'very savvy in terms of their social media,'" which should have made it much easier for the Government Defendants to track down terrorists without searching our records through the Section 215 illegal government surveillance. *See id.* As such, the Government Defendants' techniques are clearly not working and there is no justification for them to illegally search Plaintiffs' and all Americans' metadata for the mere possibility that a terrorist *might* be caught in the far future. According to the finding of the District Court, no terrorist has been so caught and there is no indication that the wholesale collection of metadata off over 300 million Americans will accomplish that objective.

CONCLUSION

In sum, this Court must respectfully affirm the District Court's Order of December 16, 2013, preliminarily enjoining the Government Defendants from continuing to illegally and unconstitutionally conduct surveillance on Plaintiffs, and hundreds of millions of Americans. Plaintiffs have never claimed that the Government Defendants are not entitled to conduct legitimate surveillance of communications of

terrorists and criminals where there is a showing of probable cause. However, as Chief Justice John Roberts of the Supreme Court has confirmed, warrantless searches of ordinary citizens are not only Orwellian but are also contrary to the principals on which this country was founded. Plaintiffs do not dispute that, under the law, the NSA may conduct surveillance on persons where there is reasonable suspicion that they are in communication with terrorists or committing crimes. What the NSA has been doing unlawfully is accessing telephony metadata of not only Plaintiffs, but hundreds of millions of Americans, that clearly exceeds Constitutional protections.

The Government Defendants' illegal surveillance of Plaintiffs' and virtually all 300 million Americans has had, and will continue to have, a prominent chilling effect on the right to feel and be secure in one's own home. As stated in *Riley*, it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him. . . . If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in

digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." 134 S.Ct. at 2490-91. This is the very thing that harms the American people because such a chilling effect inhibits their speech due to the reasonable fear that the government will continue to spy on their most intimate moments.

Our Founding Father and President Thomas Jefferson famously stated, "When governments fear the people, there is liberty. When the people fear the government, there is tyranny." Similarly, Supreme Court Chief Justice John Roberts recognized the ill effects of the government overreaching of its powers and stated that "*[T]he Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself.*" The Supreme Court was well aware of these appeals when Chief Justice Roberts wrote the majority opinion in *Riley*, and in Plaintiffs' view was also in effect speaking to and providing precedent to this Court to

decide these appeals accordingly. Thus, the Supreme Court shut the door on the Government Defendants' arguments herein.

In ruling on these appeals, this Court should respectfully take heed of the national interest, as this is perhaps the most important case to come before this Court in its history.

In sum, Plaintiffs want to preserve the status quo by simply having the Government Defendants be ordered to obey the law, which will ultimately not harm anyone. Plaintiffs and the American people thus look to this Court for their salvation.

Dated: October 3, 2014 Respectfully submitted,

/s/ *Larry Klayman*
LARRY KLAYMAN, ESQ.
Attorney at Law
D.C. Bar No. 334581
2020 Pennsylvania Ave. NW,
Suite 345
Washington, DC 20006
Tel: (310) 595-0800
Email: leklayman@gmail.com

CERTIFICATE OF COMPLIANCE WITH FEDERAL RULE OF APPELLATE PROCEDURE 32(A)

I hereby certify that that this brief complies with the requirements of Federal Rules of Appellate Procedure 32(a) and 32(a)(7) because it has been prepared in 14-point Century Schoolbook, a proportionally spaced font, and is double-spaced (except for headings and footnotes).

I further certify that this brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B) because it contains 6,979 words excluding the parts of the brief permitted to be exempted, according to the count of Microsoft Word. The words of the Reply Brief of Appellees/Cross-Appellants do not exceed 7,000 words, as mandated by Federal Rule of Appellate Procedure 32(a)(7)(B)(ii).

/s/ *Larry Klayman*
LARRY KLAYMAN, ESQ.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 3rd day of October, 2014, I filed a true and correct copy of foregoing Reply Brief of Appellees/Cross-Appellants with the Clerk of the United States Court of Appeals for the District of Columbia Circuit. All participants in the case are registered CM/ECF users and will be served by the appellate CM/ECF system. I further certify that I will cause eight (8) paper copies of this brief to be filed with the Court within two business days.

Respectfully submitted,

/s/ *Larry Klayman*
LARRY KLAYMAN, ESQ.
Attorney at Law
D.C. Bar No. 334581
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006
Tel: (310) 595-0800
Email: leklayman@gmail.com