[NOT YET SCHEDULED FOR ORAL ARGUMENT]

Nos. 04-5004, 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

BRIEF FOR PLAINTIFFS-APPELLEES AND REQUEST FOR ORAL ARGUMENT

LARRY E. 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

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

A. Parties

The appeals to the United States Court of Appeals to the District of Columbia Circuit (the "Court") herein have been consolidated from two related United States District Court for the District of Columbia (the "District Court") cases, *Klayman v. Obama*, Civ. No. 13-0851 (Nos. 14-5004, 14-5016 in this Court) ("*Klayman I*") and *Klayman v. Obama*, Civ. No. 13-0881 (14-5005, 14-5017 in this Court) ("*Klayman II*").

In *Klayman I*, Larry Elliot Klayman ("Klayman"), Charles Strange ("Mr. Strange"), and Mary Ann Strange ("Mrs. Strange") are Plaintiffs-Appellees/Cross-Appellants. Barack Hussein Obama ("Obama"), Eric H. Holder Jr. ("Holder"), Michael S. Rogers ("Rogers"), National Security Agency ("NSA"), and U.S. Department of Justice ("DOJ") are Defendants-Appellants (collectively "Government Defendants"). The United States Court of Appeals for the District of Columbia Circuit (the "Court") has consolidated Nos. 14-5004 and 14-5016 with No. 14-5005 and its cross-appeal, No. 14-5017. Nos. 14-5005 and 14-5017 are appeals from the District Court's order entered in *Klayman II*. In *Klayman II*,

Plaintiffs-Appellees/Cross-Appellants are Klayman, Michael Ferrari ("Ferrari"), Mr. Strange, Mrs. Strange, and Matt Garrison ("Garrison"). Defendants-Appellants/Cross Appellees are Holder, Obama, Rogers, NSA, and DOJ.

All above named Plaintiffs in *Klayman I* and *Klayman II* are hereinafter collectively "Plaintiffs." All above named Defendants are hereinafter collectively the "Government Defendants."

B. Ruling Under Review

The Ruling under review is Judge Richard J. Leon's Opinion and Order, dated December 16, 2013, and reported as *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013).

C. Related Cases

Two related cases to *Klayman I* and *Klayman II*, both of which are pending in the District Court challenging unlawful government surveillance, include *Klayman v. Obama*, Civ. No. 14-0092 ("*Klayman III*") and *Paul v. Obama*, Civ. No. 14-262 (D.D.C. Feb. 18, 2014). Other related cases include the United States Supreme Court's ("Supreme Court") recent decision in *Riley v. California*, 134 S.Ct. 2473 (2014), and *ACLU v. Clapper,* 959 F. Supp. 2d 724 (2014), a case filed in the

Southern District of New York and later appealed in the United States Court of Appeals for the Second Circuit ("Second Circuit") (No. 14-42 in this Court), against the Government Defendants for their unlawful use of government surveillance.

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

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

Cases

*Authorities upon which we chiefly rely are marked with asterisks.

Constitution

Statutes

GLOSSARY

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

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

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

> **"*[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.*

INTRODUCTION

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. However, what the NSA has been doing unlawfully is accessing telephony metadata of not only Plaintiffs, but hundreds of millions of Americans, that clearly exceeds Fourth, First, and Fifth Amendment protections, which is both illegal and criminal. Also, all attorneys, including Klayman and the ACLU, under a higher standard, are entitled to protection from unlawful government surveillance as the Government Defendants' access to their communications with clients and other attorneys, via telephone and email, violates their attorney-client privilege. To protect the rights of Plaintiffs and the American people, this Court must respectfully uphold the District Court's

preliminary injunction that simply requires the NSA to obey the law. Plaintiffs ultimately want to preserve the status quo, which will not harm anyone.

In *Riley v. California*, 134 S.Ct. 2473 (2014), a recent landmark Supreme Court decision that invalidates the Supreme Courts' previous ruling in *Smith v. Maryland*, 442 U.S. 735 (1979) in the context of this case, Chief Justice John Roberts spoke, and acknowledged the importance and advancement of today's phone technologies and metadata. 134 S.Ct. at 2489. This is not a pen register, this is metadata; it is every aspect of our lives. 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 id.* at 2489-93. The Supreme Court found that "[M]odern cell phones are not another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life[.]" *Id.* at 2496.

The Supreme Court in *Smith* 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. 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 unconceivable circumstances of today.

The District Court has been thoroughly familiar with this case and its current procedural posture, and has appreciated both the importance of the constitutional questions presented and the national security interests at stake. *See Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013).[1] As the District Court previously ruled, the constitutional issues raised in this case are "at the pinnacle of public national interest." The District Court found that the Government

[1] The Government Defendants inadvertently failed to include the the District Court's memorandum opinion, dated December 16, 2014, in the original appendix. Plaintiffs will be moving on August 14, 2014 to supplement the appendix, presumably with the Government Defendants' consent.

Defendants' illegal government surveillance of bulk telephony metadata surely "infringes on 'that degree of privacy' that the Founders enshrined . . . ," and that it "cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than [the] systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval." Undoubtedly, the case before us is of extreme national importance.

In this appeal, this Court must respectfully uphold the District Court's decision to issue a preliminary injunction barring the Government Defendants from collecting, as part of NSA's illegal government surveillance of bulk telephony metadata, any telephony metadata associated with their personal Verizon accounts and requiring the Government Defendants to destroy any such metadata in its possession that was collected through the illegal government surveillance. Further, this Court must respectfully reverse the District Court's decision to deny Plaintiffs' request for a preliminary injunction in *Klayman II* to preserve the status quo.

The Government Defendants have violated Plaintiffs' constitutional rights as a result of their illegal use of electronic

surveillance, as set forth in the complaints in *Klayman I* and *Klayman II*. Plaintiffs requested monetary, declaratory, equitable, and injunctive relief as a result of these unlawful acts.

The District Court properly concluded that Plaintiffs have standing to challenge the Section 215 illegal government surveillance of bulk telephony metadata because Plaintiffs do not merely speculate that the Government Defendants searched their telephony metadata, and Plaintiffs suffered injury. The District Court also properly concluded that Plaintiffs are likely to succeed on their Fourth Amendment claim because the Section 215 illegal government surveillance constitutes a search, which is unreasonable under the Fourth Amendment. In properly balancing the equities and assessing the public interest to issue a preliminary injunction, the District Court did not abuse its discretion.

The District Court, however, erred in denying Plaintiffs' request for preliminary injunction in *Klayman II* because the Government Defendants, whose repetitive conduct has demonstrated a lack of trustworthiness, have not discontinued the Section 215 illegal government surveillance as they allege, and because Plaintiffs have

provided sufficient evidence (the same amount of evidence provided in *Klayman I*) to show that the NSA has targeted Plaintiffs' Internet Data Content. These public disclosures include, but are not limited to, Edward Snowden's revelations, sworn affidavits, the District Court's opinion, the Government Defendants themselves, a plethora of newspaper and online articles, and statements made by individuals with direct contact to government officials. The District Court also erred in denying injunctive relief to Mrs. Strange because as pleaded she is also a subscriber of Verizon at all times relevant to this lawsuit. Lastly, Plaintiffs respectfully request that this Court reach a decision regarding Plaintiffs' First and Fifth Amendment Claims.

Plaintiffs understand the extreme importance of national security. At the same time, Plaintiffs also understand the extreme importance of protecting citizens' privacy, as the Founding Fathers enshrined in the U.S. Constitution. Accordingly, this degree of privacy must be protected by upholding the District Court's decision to issue a preliminary injunction. As such, due to the extreme constitutional importance of this case, Plaintiffs request that this Court uphold the District Court's decision to grant a preliminary injunction in *Klayman I* and reverse the

District Court's decision to deny Plaintiffs' request for a preliminary injunction in *Klayman II*. This Court must also respectfully remove the stay that the District Court ordered pending appeal so that the District Court's preliminary injunction can go into full force and effect.

JURISDICTIONAL STATEMENT

Plaintiffs invoked the District Court's jurisdiction under 28 U.S.C. § 1331. *See* Appendix ("App.") 39, 74. On December 16, 2013, the District Court entered an order granting in part Plaintiffs' Motion for Preliminary Injunction in *Klayman I* and denying in part Plaintiffs' Motion for Preliminary Injunction in *Klayman II*. *Klayman v. Obama*, 957 F. Supp. 2d 1, 9-10 (D.D.C 2013). The District Court entered an order "that (1) bars the Government [Defendants] from collecting, as part of NSA's illegal government surveillance of bulk telephony metadata, any telephony metadata associated with their personal Verizon accounts and (2) requires the Government [Defendants] to destroy any such metadata in its possession that was collected through the "illegal government surveillance." App. 43. The District Court stayed its order pending appeal. App. 587.

The Government Defendants filed a notice of appeal on January 3,

2014. Under 28 U.S.C. § 1292(a)(1), this Court has appellate jurisdiction to review the District Court's order partially granting and partially denying injunctive relief.

ISSUES PRESENTED FOR REVIEW

1. Whether the Government Defendants' collection of Plaintiffs' telephony metadata violates the Fourth Amendment.

2. Whether the District Court erred in granting in part Plaintiffs' Motion for Preliminary Injunction in *Klayman I*.

3. Whether the District Court erred in denying in part Plaintiffs' Motion for Preliminary Injunction in *Klayman II*.

4. Whether the District Court erred in denying injunctive relief to Mary Ann Strange.

5. Whether the Government Defendants' collection of Plaintiffs' and citizens' metadata violates the First and Fifth Amendments.

STATEMENT OF THE CASE

Plaintiffs cannot confirm that any changes to the Section 215 illegal government surveillance of bulk telephony metadata, allegedly further enhancing the illegal government surveillance's privacy protections and safeguards, were in fact adopted by the Foreign

Intelligence Surveillance Court (the "FISC"). *See* Gov't App. Brief p. at 5. Additionally, the FISC automatically grants the Government Defendants' warrants to collect metadata, and thus, there are no occasions where the Government Defendants' "requisite factual showing" resulted in a FISC judge's denial of an entry of a requested ex parte order or a disapproval of the release of tangible things. *See id.* at 7-8. The Government Defendants contend that "[f]uther review is [ ] available in the [FISA] Court of Review and, ultimately, in the Supreme Court." *See id.* at 8. However, only denials of the Government Defendants' warrant requests are appealable.

Defendants allege that the production of all call detail records of all persons in the United States has never occurred under the illegal government surveillance because production of all these call records has occurred. *See id.* at 10. Further, the District Court's correct conclusions that the illegal government surveillance collects "the phone metadata of every telephone user in the United States" and that "all phone companies" participate in the Section 215 illegal government surveillance is in fact supported by the record. *See id.* The District Courts conclusions are correct. *See id.* at 11.

The Government Defendants do not use the Section 215 illegal government surveillance merely as a tool to facilitate counterterrorism investigations—the Government Defendants also use the illegal government surveillance to unlawfully spy on American citizens without a warrant. *See id.* The Government Defendants, through querying, obtain telephones and other metadata even when a selector, such as a telephone number, is not reasonably suspected of being associated with a terrorist organization. *See id.* at 11, 14. Plaintiffs dispute that the telephony metadata returned from a query do not include the identities of individuals; the content of any calls; or the name, address, financial information, or cell site locational information of any telephony subscribers or parties to the call, because the metadata obtained under the illegal government surveillance allegedly does not contain such information. *See id.* at 14-15. The metadata does contain this information, and, in fact, names of individuals can easily be discovered using the illegal government surveillance.

The illegal government surveillance is not subject to a rigorous regime of safeguards and oversight as the Government Defendants allege. *See id.* at 16. Plaintiffs have not been able to engage in discovery

and thus cannot confirm most of the Government Defendants' statements and allegations pertaining to the illegal government surveillance, including their handling of Plaintiffs' and citizens' metadata. Plaintiffs, the District Court, Congress, and other courts, do know, however, that the Government Defendants have been untruthful in a number of occasions regarding the illegal government surveillance's collection of metadata.

Plaintiffs in *Klayman I* and *Klayman II* have been, and are, in fact subscribers of Verizon at all times relevant to this case.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

On June 5, 2013, *The Guardian*, a British newspaper, reported the first materials leaked by former NSA contract employee Edward Snowden that revealed the existence of U.S. government intelligence collection and illegal government surveillance. *See* Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, GUARDIAN (London), June 5, 2013; *see also* Leon Memorandum Opinion, dated Dec. 16, 2013 ("SA") at 6. *The Guardian's* report disclosed a secret FISC order, dated April 25, 2013, that required Verizon Business Network Services to produce to the NSA on "an ongoing daily basis . . .

all call detail records or 'telephony metadata' create by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." Secondary Order, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc. d/b/a/ Verizon Business Services*, No. BR 13-80 at 2 (FISC Apr. 25, 2013) ("Secondary Order"); Supplemental Appendix ("SA") 6.

The Secondary Order "show[ed] . . . that under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk—regardless of whether they are suspected of any wrongdoing." Greenwald, *supra*; SA 6-7. The Government Defendants confirmed the authenticity of the Secondary Order as well as the existence of the illegal government surveillance under which "the FBI obtains orders from the FISC pursuant to Section 215 [of the USA PATRIOT Act] directing certain telecommunications service providers to produce to the NSA on a daily basis electronic copies of 'call detail records.'" Govt.'s Opp'n at 8; SA 7. The illegal government surveillance is "a 'counterterrorism [illegal government

surveillance]' under [50 U.S.C. §] 1861[, conducted for more than seven years, that] collect[s], compiles, retains, and analyzes certain telephony records, which it characterizes as 'business records' created by certain telecommunications companies." SA 15-16. The illegal government surveillance is "meant to detect: (1) domestic U.S. phone numbers calling outside of the United States to foreign phone numbers associated with terrorist groups; (2) foreign phone numbers associated with terrorist groups calling into the U.S. to U.S. phone numbers; and (3) 'possible terrorist –related communications' between numbers inside the U.S." SA 20-21.

The records collected under the illegal government surveillance consist of "metadata," which includes information about what phone numbers were used to make and receive calls, when the calls took place, and how long the calls lasted. App. 203. Through targeted searches of metadata records, the NSA "tries to discern connections between terrorist organizations and previously unknown terrorist operatives located in the United States." SA 16. The telephone metadata records, which "[telecommunications] companies create and maintain as part of their business of providing telecommunications services to customers[,]"

have been continually produced since May 2006 under the FBI's production orders from the FISC. *See* SA 16. The NSA then consolidates the metadata records provided by different telecommunications companies into one database and under the FISC's orders, the NSA may retain the records for up to five entire years. SA 16. When an NSA intelligence analyst runs a query, the quantity of phone numbers captured is very large, potentially and sometimes up to 1,000,000 numbers total. SA 18-19.

Since the illegal government surveillance began in May 2006, the FISC has regularly issued orders directing telecommunication service providers to produce records in connection with the illegal government surveillance. SA 21. Fifteen different FISC judges have issued thirty-five orders authorizing the illegal government surveillance and under those orders, the Government defendants must continuously seek renewal of the authority to collect telephony records, which occurs every ninety days. SA 21. The Government Defendants admit that they have failed to comply with the minimization procedures set forth in the orders. SA 21. Judge Reggie Walton of the FISC concluded he had no confidence that the Government was doing its utmost to comply with

the court's orders. SA 21-22. Judge John Bates, Presiding Judge of the FISC, found that the Government had misrepresented the scope of its targeting of certain internet communications pursuant to 50 U.S.C. § 1881a. SA 22. The Government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which he Government disclosed a substantial misrepresentation regarding the scope of a major illegal government surveillance collection. SA 23.

After the public revelations of the Government Defendants' secret schemes in the media, Plaintiffs filed their first complaint, *Klayman I*, on June 6, 2013. *See* SA 8. *Klayman I* Plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange, all subscribers of Verizon Wireless, brought suit against the NSA, the DOJ, multiple executive officials, whom include President Barack H. Obama, Attorney General Eric H. Holder, Jr., General Keith B. Alexander, Director of the NSA, and U.S. District Judge Roger Vinson, and Verizon Communications as well as its chief executive officer. *See* App. 33-59; SA 8. On June 9, 2013, Plaintiffs filed an amended complaint in *Klayman I*. *See* App. 36-59. As relief, Plaintiffs sought a preliminary injunction "that, during the

pendency of this suit, (i) bars [d]efendants from collecting [p]laintiffs' call records under the mass call surveillance [illegal government surveillance]; (ii) requires [d]efendants to destroy all of [p]laintiffs' call records already collected under the [illegal government surveillance]; and (iii) prohibits [d]efendants from querying metadata obtained through the [illegal government surveillance] using any phone number or other identifier associated with [p]laintiffs . . . and such other relief as may be found just and proper." App. 56-59. Plaintiffs filed their second complaint, *Klayman II*, on June 12, 2013. *Klayman II*.

On December 16, 2013, the District Court issued its Memorandum Order in *Klayman I*. The District Court found that it had authority to evaluate Plaintiffs' constitutional challenges to the NSA's conduct. SA 5. After careful analysis of the facts, the District Court ruled that the NSA's bulk telephony metadata collection and analysis violates a reasonable expectation of privacy, SA 47, and thus, the NSA's illegal government surveillance is an unreasonable search under the Fourth Amendment. SA 62. To determine whether the District Court should grant Plaintiffs' request for a preliminary injunction, the District Court concluded that "Plaintiffs have standing to challenge the

constitutionality of the Government's bulk collection and querying of phone record metadata, that they have demonstrated a substantial likelihood of success on the merits of their Fourth Amendment claim, and that they will suffer irreparable harm absent preliminary injunctive relief." SA 5. The District Court also concluded that the public interest weighs heavily in favor of granting an injunction. SA 65. Accordingly, the District Court granted the Motion for Preliminary Injunction in *Klayman I*. App. 586. The District Court determined that it would stay its order pending appeal. *Id*. On January 3, 2014, the Government Defendants filed a notice of appeal.

On February 3, 2014, in a hearing before the District Court, Plaintiffs orally reiterated their consideration for streamlining the cases and moving as quickly as possible because, as Plaintiffs stated, "when constitutional rights are violated for one minute, that's one minute too long . . . ." Transcript, Hearing, 11:12-16 (Feb. 3, 2014).

On June 25, 2014, the Supreme Court issued *Riley* and held that "[t]he police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." Chief Justice John Roberts found, in the majority opinion,

that the Supreme Court's decision would "have an impact on the ability of law enforcement to combat crime," that cell phones are essentially "minicomputers" that "also happen to have the capacity to be used as a telephone," and that "[p]rivacy comes at a cost." *Riley*, 134 S.Ct. at 2493. The Supreme Court also 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 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 further ruled that "a warrant is generally required before [ ] a search, even when a cell phone is seized incident to arrest." *Id.* at 2493. 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.

The fact that internet metadata, in addition to telephony metadata, both of which are accessible on a cell phone, is at issue here, makes the present case even more compelling. Indeed, the Supreme Court's decision will have a substantial impact on the outcome of this case, as it further adds to the fact that the Government Defendants' Fourth Amendment search of Plaintiffs' metadata is unreasonable. In fact, *Riley,* in the context of this case, eliminates *Smith*. This is not a pen register, this is metadata; it is every aspect of our lives.

SUMMARY OF THE ARGUMENT

The District Court properly granted Plaintiffs' Motion for Preliminary Injunction by finding that Plaintiffs were likely to succeed on the merits of their Fourth Amendment claim against the Government Defendants, and this Court should respectfully affirm the District Court's decision. The District Court found that the Government Defendants' surveillance constituted an unreasonable search when they illegally obtained the telephony and Internet metadata records of Plaintiffs and all Americans.

Further, the District Court erred in denying a preliminary injunction in *Klayman II*. Plaintiffs had demonstrated standing and

provided sufficient evidence to show that the NSA targeted Plaintiffs' internet data content. Thus, this Court should respectfully reverse the District Court's decision to deny Plaintiffs' Motion for Preliminary Injunction.

Finally, this Court should respectfully reach a decision on Plaintiffs' First and Fifth Amendment claims because these claims are just as important as Plaintiffs' Fourth Amendment claim in protecting Plaintiffs' rights.

STANDARD OF REVIEW

This Court "review[s] a District Court's weighing of the four preliminary injunction factors and its ultimate decision to issue or deny such relief for abuse of discretion." *David v. Pension Ben. Guar. Corp.*, 571 F.3d 1288, 1291 (D.C. Cir. 2009) "Legal conclusions—including whether the movant has established irreparable harm—are reviewed *de novo*." *Id.*

ARGUMENT

I. THE DISTRICT COURT PROPERLY ENTERED A PRELIMINARY INJUNCTION AGAINST THE OPERATION OF THE SECTION 215 ILLEGAL GOVERNMENT SURVEILLANCE OF BULK TELEPHONY METADATA.

A. The District Court Properly Concluded That Plaintiffs Have Standing To Challenge The Section 215 Illegal Government Surveillance Of Bulk Telephony Metadata.

As the District Court correctly ruled, Plaintiffs have successfully demonstrated that the Government Defendants collected Plaintiffs' telephony metadata without speculation, and the Government Defendants will continue to do so unless the preliminary injunction is upheld.[2] Plaintiffs have suffered injury as a result of the Government Defendants' unlawful activity.

"To establish Article III standing, an injury must be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1147 (2013) (quoting *Monsanto Co.*

[2] Plaintiffs in this case can point to strong evidence that, as Verizon customers, their telephony metadata has been collected for the last seven years (and stored for the last five) and will continue to be collected barring judicial or legislative intervention. *See* App. 343 - Suppl. Klayman Aff. ¶ 3 (attesting to status as Verizon customer); App. 101 - Strange Aff. ¶ 2 (same).

v. Geertson Seed Farms, 561 U.S. 139, 149 (2010)). "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending." *Clapper*, 133 S.Ct. at 1147 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 565 n.2 (1992)).

Under the circumstances of this case, the District Court ruled that Plaintiffs have standing to challenge the NSA's Bulk Telephony Metadata collection and analysis. *See* SA 36. The District Court held that "[P]laintiffs have standing to challenge both" of the NSA's illegal government surveillance of bulk telephony metadata's two potential searches: (1) the bulk collection of metadata and (2) the analysis of that data through the NSA's querying process." SA 36.

1. Plaintiffs Do Not Merely Speculate That Their Telephony Metadata Has Been Searched As A Result Of The Section 215 Illegal Government Surveillance.

The District Court properly ruled that the Government Defendants have searched Plaintiffs' metadata. Plaintiffs and the District Court are well aware that their telephony metadata has been searched by the Government Defendants. In fact, everyone's metadata

has been searched, as concluded by the District Court. In determining whether Plaintiffs met the requirements for standing, the District Court analyzed *Clapper* and ultimately ruled that the facts that arise in Plaintiffs claims are distinguishable from *Clapper*.[3] In *Clapper*, where the plaintiffs "could only speculate as to whether they would be surveilled at all, [P]laintiffs in [*Klayman I*] can point to strong evidence that, as Verizon customers, their telephony metadata has been collected for the last seven years (and stored for the last five) and will continue to be collected barring judicial or legislative intervention." 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

[3] "In *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), the Supreme Court held that plaintiffs lacked standing to challenge NSA surveillance under FISA because their 'highly speculative fear' that they would be targeted by surveillance relied on a 'speculative chain of possibilities' insufficient to demonstrate a 'certainly impending' injury. *Id.* at 1147–50. Moreover, the *Clapper* plaintiffs' 'self-inflicted injuries' (i.e., the costs and burdens of avoiding the feared surveillance) could not be traced to any provable government activity. *Id.* at 1150–53.33." That is not the case here. SA 26.

will continue to operate the illegal government surveillance consistent with FISC opinions and orders."[4] SA 42.

The Government Defendants attempt to argue that Plaintiffs' claim to injury is based only on speculation because Plaintiffs "express concern that their communications will be 'overheard or obtained' under the Section 215 [illegal government surveillance]" and that "there is no evidence that the Government Defendants collected any information about Plaintiffs' calls under the [illegal government surveillance]." It is important to point out, however, that the Government Defendants have not denied collecting information about Plaintiffs' calls.

Under the Government Defendants' disingenuous if not false legal arguments, no Plaintiff could successfully allege injury absent concrete evidence that their particular metadata had been searched, which is nearly impossible because the Government Defendants refuse to hand over any information or relevant documents, and they refuse to engage in a Fed. R. Civ. P. Rule 26(f) discovery conference, much more participate in responding to any subsequent discovery requests. The individual Defendants refused to even respond to the Complaint,

[4] The District Court found that Plaintiffs have standing to challenge the NSA's querying procedures. SA 38.

despite being duly served in *Klayman I* and *Klayman II*. If this Court were to accept the Government Defendants' arguments alleging Plaintiffs' supposed lack of standing, which the District Court has previously denied,[5] then any person who "seek[s] to challenge the surveillance [illegal government surveillance] will be caught in a nearly impossible conundrum . . . ." *See* Leighton Woodhouse, *Is The Government Lying About How Much Of Your Metadata It's Using?*, Huffington Post (Aug. 15, 2013), available at http://www.huffingtonpost.com/2013/08/15/government-metadata_n_3762050.html.

Plaintiffs would "need to show that their metadata was swept up in an NSA query, a task that requires access to state secrets. Unless the government were to take the unlikely step of granting the opposing counsel the necessary security clearances to acquire this evidence, the standard for achieving standing would be virtually impossible to meet."[6]

---

[5] *See* SA 36.

[6] "Even this scenario, however, puts control of the process largely in the [G]overnment's hands, as federal prosecutors [or the Government Defendants] are able to decide whether to press charges and whether to use the NSA-derived evidence, weighing the benefits of doing so against the risk of inviting a challenge to the [illegal government] surveillance [ ]." Woodhouse, Huffington Post, *supra*. "If federal prosecutors [or the

Id. 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.

Even if, for instance, there was no concrete proof that Plaintiffs' exact metadata had been searched at a given time, 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

---

Government Defendants] can avoid using NSA-derived evidence . . . , and if their argument on standing is upheld by the courts, then the government can indefinitely forestall any possibility of a plaintiff meeting the "actual and imminent harm" standard. And if the standard for achieving standing is unattainable, then the [illegal government surveillance] [is] effectively immunized from Constitutional challenge." *Id.*

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 an historical repository that permits retrospective analysis of terrorist-related communications *across multiple telecommunications networks,* and that can be immediately accessed as new terrorist-associated telephone identifiers come to light.'" SA 27. Accordingly, the District Court ruled "the NSA *must* have collected metadata from Verizon Wireless."

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 must have been 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. 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 are aware that Plaintiffs' telephony metadata has been searched.

For the foregoing reasons, the District Court correctly concluded that Plaintiffs did not merely speculate that their telephony metadata records were searched.

2. The Section 215 Illegal Government Surveillance Inflicted Injury On Plaintiffs Sufficient To Support Standing.

In concluding that Plaintiffs had standing to challenge the unlawful use of the illegal government surveillance, the District Court also correctly ruled that Plaintiffs were injured when the Government Defendants collected and searched their information.

Whether the Government Defendants actually "reviewed" Plaintiffs' information is irrelevant to the issue of finding injury for standing. The District Court held that "[P]laintiffs suffer a constitutionally cognizable injury each time the government electronically queries the Section 215 database because '[P]laintiffs' metadata . . . is analyzed, manually or automatically' whenever an electronic query of the database is run—even if plaintiffs' metadata is never seen by any human being as part of a query result." *DaimlerChrysler Corp.* v. *Cuno*, 547 U.S. 332, 345 (2006). As such, Plaintiffs suffer a cognizable Article III injury each time the government queries the database, because all information in the database is analyzed when the Government runs a query. 957 F. Supp.

2d at 28. Even in the unlikely event where "queries of the database [ ] return no information about plaintiffs," Plaintiffs would still be harmed. Use of Plaintiffs' records only aggravates the original injuries inflicted upon Plaintiffs when their data is searched. *See, e.g.*, *Nat'l Ass'n of Letter Carriers, AFL–CIO v. U.S. Postal Serv.*, 604 F. Supp. 2d 665, 675 (S.D.N.Y. 2009) (Chin, J.) (holding that postal employees had standing to bring suit under the Fourth Amendment where they challenged the government's collection of their medical records from health-care providers); *see also Amidax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140 (2d Cir. 2011) (observing that a plaintiff seeking to establish standing to challenge government surveillance "need only establish that its information was obtained by the government.")).

The Government Defendants have contended that there exists no case or controversy unless Plaintiffs' records are actually *responsive* to one of the government's queries. In their appellate brief to the Second Circuit, the ACLU has addressed this seemingly popular yet meritless argument by the Government Defendants. The ACLU correctly pointed out that not only is "the government's argument that there is no case or controversy until an analyst "reviews" the information the government

has collected . . . simply wrong, [it is] radically so." In reaching this determination, the ACLU argued that that "[i]f the collection of information could not give rise to a case or controversy, the Constitution would permit the government to copy every email, record every phone call, and make a permanent record of every person's physical movements—all without ever having to justify its actions to any court [and] [t]he Constitution would be engaged, if at all, only when the government decided to review the data it had collected." In other circumstances, responsiveness was not relevant in determining whether case or controversy exists. For example, as the ACLU provided, "[a] person whose luggage is inspected has been searched even if the inspection turns up no contraband. A person whose home is subjected to thermal-imaging has been searched even if the scan does not show that the person is growing marijuana." *Cf. Kyllo v. United States*, 533 U.S. 27 (2001). "Whether a search has occurred—and, certainly, whether an Article III injury has been inflicted—does not turn on whether the search produces information that the government regards as useful or incriminating." ACLU Appellate Brief at p.4 n.2.

For the aforementioned reasons, the District Court correctly concluded that Plaintiffs have successfully shown that their metadata has been searched by the Government Defendants, and that Plaintiffs have been injured as a result of this search. Thus, Plaintiffs have standing to pursue their Fourth Amendment claim against the Government Defendants.

B. The District Court Properly Concluded That Plaintiffs Are Likely To Succeed On Their Claim That The Section 215 Illegal Government Surveillance Violates The Fourth Amendment.

"The basic purpose of th[e Fourth] Amendment, as recognized in countless decisions of th[e] [Supreme] Court, is to safeguard the privacy and security of individuals against *arbitrary invasions by governmental officials*." *Camara v. Mun. Court,* 387 U.S. 523, 528 (1967) (emphasis added); *see also Quon,* 130 S. Ct. at 2627 ("The Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government, without regard to whether the government actor is investigating crime or performing another function." (internal quotation marks omitted)).

The District Court properly found that Plaintiffs' Fourth

Amendment arguments are most likely to succeed because the Section 215 illegal government surveillance violates the Fourth Amendment. In reaching this decision, the District Court correctly concluded that the illegal government surveillance is an unreasonable search under the Fourth Amendment.

1. The Section 215 Illegal Government Surveillance of Telephony Metadata Constitutes A Search Under the Fourth Amendment.

The District Court ultimately found that Plaintiffs made more than "a sufficient showing to merit injunctive relief on their Fourth Amendment claim." SA 5 n.7. In analyzing the first prong to determine the existence of a Fourth Amendment violation, the District Court found that a Fourth Amendment search had occurred, and "[P]laintiffs have a very significant expectation of privacy in an aggregated collection of their telephony metadata covering the last five years, and the NSA's illegal government surveillance of bulk telephony metadata significantly intrudes on that expectation." *Id.* at 58-59.

In *Riley*, a recent landmark Supreme Court decision that invalidates the Supreme Courts' previous ruling in *Smith v. Maryland*, 442 U.S. 735 (1979) in the context of this case, Chief Justice John

Roberts spoke, and acknowledged the importance and advancement of today's phone technologies and metadata. *See Riley* v. *California*, 134 S. Ct. 2473, 2489 (2014) (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; it is every aspect of our lives.

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.[7] *Id.* at 2495. Because "[d]igital data stored on a cell phone cannot itself be used as a

[7] "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant." *Riley*, 134 S.Ct. at 2494 (emphasis added).

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 *Smith* 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,[8]

[8] "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.

when *Chimel*[9] and *Robinson*[10] 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 unconceivable circumstances of today.

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 necessarily applicable as the Supreme Court justices in 1979 could not have

---

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.

[9] 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 plethora of information found in one's cell phone is equivalent to the amount of information one can find from searching one's home. The Government Defendants are thus bursting into the homes of everyone.

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

envisioned the full extent that, or how, technology would advance.[11]

In *Smith,* police were investigating a robbery victim's reports that she had received threatening and obscene phone calls from someone claiming to be the robber. *Id.* at 737, 99 S.Ct. 2577. Without obtaining a warrant or court order, police installed a pen register, which revealed that a telephone in Smith's home had been used to call the victim on one occasion. *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

---

[11] "[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." "The notion that the Government could collect similar data on hundreds of millions of people and retain that data for a five-year period, updating it with new data every day in perpetuity, was at best, in 1979, the stuff of science fiction." SA 49.

bulk telephony metadata is not a search. Govt.'s Opp'n at 45–50. In 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, when do present-day circumstances, namely the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies, that have become so thoroughly unlike those considered by the Supreme Court in 1979 that a precedent like *Smith* would not apply? The District Court simply answered, "now."[12] Consequently, the District Court ruled that the bulk telephony metadata collection and analysis almost certainly does violate a

[12] Judge Leon concluded, "I am convinced that the [illegal government surveillance] now before me is so different from a simple pen register that *Smith* is of little value in assessing whether the [illegal government surveillance] of [b]ulk [t]elephony [m]etadata constitutes a Fourth Amendment search." SA 47.

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),[13] 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."[14] 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

[13] "In his affidavit, Acting Assistant Director of the FBI Robert J. Holley himself noted that "[p]en-register and trap-and-trace (PR/TT) devices provide no historical contact information, only a record of contacts with the target occurring after the devices have been installed." App. 223.

[14] "And I might add, there is the very real prospect that the [illegal government surveillance] will go on for as long as America is combatting terrorism, which realistically could be forever!" SA 47.

telecom companies.[15] 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

---

[15] *Compare Smith,* 442 U.S. at 737 ("[T]he telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at petitioner's home."), *with* Govt.'s Opp'n at 8–9 ("Under this [illegal government surveillance], . . . certain telecommunications service providers [ ] produce to the NSA *on a daily basis* electronic copies of call detail records, or telephony metadata. . . . The FISC *first authorized the [illegal government surveillance] in May 2006,* and since then has renewed the [illegal government surveillance] thirty-five times . . . ." (emphases added; citation and internal quotation marks omitted)).

relationship with phones than they did in 1979.[16] *See Klayman*, 957 F. Supp. 2d at 36. 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.* The District Court correctly pointed out that cell phones today are used as far more than just calling devices; they are also used, for example, as "maps and music players," or as a "lighter[] that people hold up at rock concerts." *Id.* at 34.

"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. Trends have resulted in a *greater* expectation

---

[16] "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). In December 2012, there were a whopping 326,475,248 mobile subscriber connections in the United States, of which approximately 304 million were for phones. CTIA—The Wireless Ass'n ("CTIA"), *Wireless Industry Survey Results—December 1985 to December 2012,* at 2, 6 (2013) ("CTIA *Survey Results* ").

of privacy and a recognition that society views that expectation as reasonable. In analyzing whether Plaintiffs have a reasonable expectation of privacy that is violated when the Government Defendants collected and searched their telephony metadata,[17] the District Court determined that it was significantly likely it would answer in Plaintiffs' favor. The District Court found that the "[P]rogram infringes on '[the] degree of privacy' that the Founders enshrined in the Fourth Amendment," SA 64, and subsequently "grant[ed] Plaintiffs requests for a[ ] [preliminary] injunction[.]" *Id.*

The District Court determined it would ultimately have to answer "whether people have a reasonable expectation of privacy that is violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-tech querying and analysis without any case-by-case judicial approval." SA 56. The District Court stated it was significantly likely that it would answer that question in Plaintiffs' favor. *Id.*

[17] "The more difficult question, however, is whether their expectation of privacy is one that society is prepared to recognize as objectively reasonable and justifiable." SA 55.

As such, a Fourth Amendment search has occurred and the ruling in *Smith* does not foreclose Plaintiffs' arguments. In any event, the Supreme Court's recent landmark holding in *Riley* renders *Smith* inoperative and obsolete, particularly in the context of this case.

2. The Section 215 Illegal Government Surveillance Of Telephony Metadata Is An Unreasonable Search Under the Fourth Amendment.

The Government Defendants' collection of bulk telephony metadata from the business records of telecommunications companies constitutes a Fourth Amendment search that is constitutionally impermissible.

After finding that a Fourth Amendment searched occurred, a district court must then must "examin[e] the totality of the circumstances to determine whether [the] search is reasonable within the meaning of the Fourth Amendment." *Samson v. California*, 547 U.S. 843, 848 (2006). " '[A]s a general matter, warrantless searches are *per se* unreasonable under the Fourth Amendment.' " *Nat'l Fed'n of Fed. Emps.–IAM v. Vilsack,* 681 F.3d 483, 488–89 (D.C.Cir.2012) (quoting *Quon,* 130 S.Ct. at 2630); *see also Chandler v. Miller,* 520 U.S. 305, 313

(1997) ("To be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing.").

"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)). A suspicionless search may still be reasonable "'where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion.'" SA 57 (quoting *Skinner,* 489 U.S. at 624).

A district court has the task of " 'balanc[ing] the [plaintiffs'] privacy expectations against the government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context.'" SA 57 (quoting *Nat'l Treasury Emps. Union v. Von Raab,* 489 U.S. 656, 665–66 (1989)). This is a " 'context-specific inquiry' " that involves " 'examining closely the competing private and public interests advanced by the parties.' " SA 57 (quoting *Chandler,* 520 U.S. at 314)). The factors the District Court

must consider include: (1) "the nature of the privacy interest allegedly compromised" by the search, (2) "the character of the intrusion imposed" by the government, and (3) "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them." *Bd. of Educ. v. Earls,* 536 U.S. 822, 830–34 (2002). Whether the illegal government surveillance violates the Fourth Amendment will therefore turn on "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them." *Earls,* 536 U.S. at 834.

The District Court explained that "special needs" cases "form something of a patchwork quilt."[18] SA 58. "To [the District Court's] knowledge, however, no court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion."

---

[18] "[S]chools and government employers are permitted under certain circumstances to test students and employees for drugs and alcohol, *see Earls,* 536 U.S. 822; *Von Raab,* 489 U.S. 656; *Skinner,* 489 U.S. 602, and officers may search probationers and parolees to ensure compliance with the rules of supervision, *see Griffin v. Wisconsin,* 483 U.S. 868 (1987). The doctrine has also been applied in cases involving efforts to prevent acts of terrorism in crowded transportation centers. *See, e.g., Cassidy v. Chertoff,* 471 F.3d 67 (2d Cir. 2006) (upholding searches of carry-on bags and automobiles that passengers bring on ferries); *MacWade v. Kelly,* 460 F.3d 260 (2d Cir. 2006) (upholding searches of bags in New York City subway system)." SA 58.

Although it is undisputed that preventing terrorist attacks is of the highest order of magnitude, the District Court correctly pointed out, however, that the Government Defendant's interest is more nuanced because it "is not merely to investigate potential terrorists, but rather to do so *faster* than other investigative methods might allow," at the expensive of citizens' and Plaintiffs' privacy. SA 59-60. In fact, the affidavits in support of the Government Defendants' brief to the District Court primarily focused on speed.[19] The Government Defendants could not cite or describe a single instance "in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government [Defendants] in achieving any objective that was time-sensitive in nature."[20] SA 61. The Government Defendants argument that the Fourth Amendment plainly does not

---

[19] "For example, according to SID Director Shea, the primary advantage of the bulk metadata collection is that "it enables the Government to *quickly* analyze past connections and chains of communication," and "increases the NSA's ability to *rapidly* detect persons affiliated with the identified foreign terrorist organizations." Shea Decl. ¶ 46 (emphases added).

[20] "In fact, none of the three 'recent episodes' cited by the Government that supposedly 'illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack' involved any apparent urgency. *See* Holley Decl. ¶¶ 24–26.

require the government to demonstrate that special-needs searches—prevented such specific harms, particularly where, as here, plaintiffs' cognizable privacy interests are minimal is unfounded because, as the District Court found, Plaintiffs' and citizens' privacy interests are not minimal—such an argument that privacy interests here are minimal disregards the importance of Fourth Amendment protection and the preventing of government tyranny.

Given the limited record and the 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 had "serious doubts about the efficacy of the illegal government surveillance as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism." Consequently, the District Court found that Plaintiffs had a substantial likelihood of showing that their privacy interests outweighed the Government Defendants' interest in collecting and analyzing bulk telephony metadata and therefore the NSA's illegal government surveillance collection of bulk metadata is indeed an unreasonable search under the Fourth Amendment.

The Supreme Court's decision in *Riley* confirms the fact that the

Government Defendants' search of Plaintiffs' telephony metadata is unreasonable. The fact that *Riley* protects arrested persons' and criminals' privacy is significant because the Government Defendants here seek to eliminate privacy protections to innocent persons and noncriminals whom have never been arrested. If, due to the amount of private and sensitive information available on a mobile phone, a police officer is required to obtain a warrant to search an arrestee's mobile phone, then, at the very least, a warrant is required to search innocent citizens' mobile phones and telephony metadata.

Accordingly, for the above stated reasons, the Government Defendants' search of Plaintiffs' telephony metadata is unreasonable under the Fourth Amendment.

C. The District Court Did Not Abuse Its Discretion In Properly Balancing The Equities And Assessing The Public Interest.

Plaintiffs have demonstrated a likelihood of success on the merits and thus the District Court did not abuse its discretion in correctly issuing a preliminary injunction.

When ruling on a motion for preliminary injunction, a district court must "'balance the [plaintiffs'] privacy expectations against the

government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context.'" *Id.* (quoting *Nat'l Treasury Emps. Union v. Von Raab,* 489 U.S. 656, 665–66 (1989)). In a "'context-specific inquiry,'" there involves "'examining closely the competing private and public interests advanced by the parties.'" SA 57 (quoting *Chandler,* 520 U.S. at 314). The factors the district court must consider include: (1) "the nature of the privacy interest allegedly compromised" by the search, (2) "the character of the intrusion imposed" by the government, and (3) "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them." *Bd. of Educ. v. Earls,* 536 U.S. 822, 830–34 (2002).

A district court does not abuse its discretion in awarding preliminary injunctive relief when balancing the equities tilts toward granting a preliminary injunction in addition to determining that plaintiffs have shown that they are likely to succeed on the merits. *Sherley v. Sebelius*, 644 F.3d 388 (D.C. Cir. 2011). "But while the standard to be applied by the district court in deciding whether a plaintiff is entitled to a preliminary injunction is stringent, the standard of appellate review is simply whether the issuance of the

injunction, in the light of the applicable standard, constituted an abuse of discretion." *Doran v. Salem Inn, Inc.*, 422 U.S. 922, 931-32 (1975) (citing *Brown v. Chote*, 411 U.S. 452, 457 (1973)).

As the U.S. Court of Appeals for the Sixth Circuit has held, "[t]he government has no legitimate interest, however, in conducting surveillance that violates both FISA and the Constitution." *Memphis Planned Parenthood, Inc. v. Sundquist*, 175 F.3d 456, 495 (6th Cir. 1999) ("[T]he public is certainly interested in preventing the enforcement of unconstitutional statutes and rules; therefore, no harm to the public will result from the issuance of the injunction here."); *see also ACLU v. Ashcroft*, 322 F.3d 240, 247 (3d Cir. 2003).

"'[I]t is always in the public interest to prevent the violation of a party's constitutional rights.'" *Am. Freedom Def. Initiative v. Wash. Metro. Area Transit Auth.,* 898 F.Supp.2d 73, 84 (D.D.C.2012) (quoting *G & V Lounge, Inc. v. Mich. Liquor Control Comm'n,* 23 F.3d 1071, 1079 (6th Cir.1994)); *see also Hobby Lobby Stores, Inc. v. Sebelius,* 723 F.3d 1114, 1145 (10th Cir.2013); *Melendres v. Arpaio,* 695 F.3d 990, 1002 (9th Cir.2012) (same); *Nat'l Fed'n of Fed. Emps. v. Carlucci,* 680 F.Supp. 416 (D.D.C.1988) ("[T]he public interest lies in enjoining

unconstitutional searches.")." The District Court determined the "interest looms large in this case, given the significant privacy interests at stake and the unprecedented scope of the NSA's collection and querying efforts, which likely violate the Fourth Amendment[, and] [t]hus, the public interest weighs heavily in favor of granting an injunction."

In arguing that the public's interest in combating terrorism is of paramount importance, which Plaintiffs and the District Court accept without question, the Government Defendants offer no real explanation as to how granting relief to Plaintiffs would be detrimental to that interest. "Instead, the Government says that it will be burdensome to comply with any order that requires the NSA to remove plaintiffs from its database." However, the public has no interest in "protecting" the Government from the burdens of complying with the Constitution. Govt.'s Opp'n at 65 (citing Shea Decl ¶ 65). For the reasons already explained, Plaintiffs and the District Court are not convinced "that the NSA's database has ever truly served the purpose of rapidly identifying terrorists in time-sensitive investigations, and so [the District Court] is *certainly* not convinced that the removal of two individuals from the

database will 'degrade' the illegal government surveillance in any meaningful sense." The District Court in no way abused its discretion as it is so alleged by the Government Defendants.

II. THE DISTRICT COURT ERRED IN DENYING IN PART PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION IN *KLAYMAN II*.

A. Plaintiffs in *Klayman II* Are Subscribers Of Verizon.

The District Court already found in *Klayman I* that Plaintiffs are subscribers of Verizon. This finding does not change the fact that Plaintiffs are still subscribers of Verizon for purposes of standing in *Klayman II*. *Klayman I* and *Klayman II* have been consolidated, which would in effect show that Plaintiffs have standing in both District Court cases.

The District Court erred, however, in deferring on ruling on the remaining motions and denying Mrs. Strange injunctive relief when Mrs. Strange has been a subscriber of Verizon at all times relevant to this case. The District Court erred in determining that Plaintiffs did not state that Mrs. Strange was a Verizon Subscriber in *Klayman II*. However, in the *Klayman II* complaint, ¶ 18, Plaintiffs state that,

"Plaintiffs Charles and Mary Ann Strange are consumers, subscribers, and users of Verizon . . . ." *See* Second Amended Complaint [Doc. 55-1].

The District Court found that Mr. Strange had standing to assert his claims along with Plaintiffs against the Government Defendants in *Klayman I*. Naturally, Mr. Strange's wife, Mrs. Strange, who lives in the same household as Mr. Strange and shares a cellular phone service with him, is also a subscriber of Verizon. Accordingly, the District Court erred in denying injunctive relief to Mrs. Strange.

B. The Government Defendants Have Not Discontinued The Section 215 Illegal Government Surveillance.

The Government Defendants contend that the illegal government surveillance, authorized under Section 215 of the FISA, used to access internet metadata and other data "was discontinued in 2011," and thus, "Plaintiffs lack standing to pursue any prospective injunctive relief." *See also* Govt. Defs.' Opp'n to Pls.' Mot. for Prelim. Inj. ("Govt.'s Opp'n") [Dkt. # 25], at 15–16, 44–45; Ex. J to Decl. of James J. Gilligan ("Gilligan Decl.") [Dkt. # 25–11] (Letter from James R. Clapper to the Sen. Ron Wyden (July 25, 2013)). Although the District Court has found it had no need to address Plaintiffs' claims requesting preliminary injunctive relief regarding any alleged internet data surveillance

activity because "the Government represented that any bulk collection of internet *metadata* pursuant to Section 215 (50 U.S.C. § 1861) was discontinued in 2011, the Government Defendants have, on a number of occasions, misrepresented their conduct before Congress and other courts, and therefore cannot be believed. The Government Defendants have offered no real proof that they discontinued the illegal government surveillance. Regardless of the Government Defendants' unfounded assertion that they discontinued the illegal government surveillance, Plaintiffs are entitled to both monetary and injunctive relief for past illegal and unconstitutional conduct.

The Government Defendants cannot be believed, as evidenced by their repetitive deceptive conduct, and thus, their assertions that they ceased accessing Internet metadata and other data through Section 215 absent discovery should not be accepted. The Government Defendants have been caught, on a number of occasions committing perjury—that is, lying to the judiciary, Congress, and the American people. The Government Defendants are dishonest: they make false representations that they have ceased accessing Internet metadata and other data through Section 215, without providing any credible or verifiable

evidence, and then they seek to dismiss Plaintiffs' claims for lack of standing so that they can avoid discovery, which would ultimately confirm further the Government Defendants' unlawful secret schemes to the public. Under this subterfuge plan, the Government Defendants intend for no party to successfully challenge the Government's violations of the U.S. Constitution.

As Plaintiffs have previously pointed out, the Government Defendants acknowledge, as they must, that they have failed to comply with the minimization procedures set forth in certain orders. SA 21. For instance, in 2009, the Government Defendants reported to the FISC that the NSA had improperly used an "alert list" of identifiers to search the bulk telephony metadata, which was composed of identifiers that had *not* been approved under the RAS standard. SA 21. Judge Reggie Walton of the FISC, who reviewed the Government Defendants' reports on their noncompliance, concluded that the NSA had engaged in "systematic noncompliance" with FISC-ordered minimization procedures over the proceeding years, since the inception of the Bulk Telephony Metadata illegal government surveillance, and had also repeatedly made misrepresentations and inaccurate statements about

the illegal government surveillance to the FISC judges. Mem. Op at 21. Judge Reggie Walton concluded that he had no confidence that the Government was doing its utmost to comply with the court's orders, and ordered the NSA to seek FISC approval on a *case-by-case basis* before conducting any further queries of the bulk telephony metadata collected pursuant to Section 1861 orders. Mem. Op at 21.

The Government Defendants have also had further compliance problems relating to its collection illegal government surveillance in subsequent years. SA 21. In 2011, the Presiding Judge of the FISC, Judge John Bates, found that the Government had misrepresented the scope of its targeting of certain internet communications pursuant to 50 U.S.C § 1881a. SA 21. Judge Bates wrote "the Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection [illegal government surveillance]." SA 21-22. In fact, since January 2009, the FISC's authorizations of the illegal government surveillance has "been premised on a flawed depiction of how the NSA uses BR metadata." SA

22 n.23. "This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime." SA 22 n.23. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively." SA 22 n.23.

The Government Defendants' plethora of misrepresentations does not stop here. Senator Ron Wyden asked James Clapper ("Clapper"), Director of National Intelligence, whether the NSA collected "any type of data at all on millions or hundreds of millions of Americans." Brian Fung, *Darrell Issa: James Clapper lied to Congress about NSA and should be fired*, Wa. Post (Jan. 27 2014), available at http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/27/darrell-issa-james-clapper-lied-to-congress-about-nsa-and-should-be-fired/. Clapper infamously replied, "No, sir … not wittingly." *Id.* Edward Snowden's revelations and leaked NSA documents forced Clapper to

admit that he knowingly lied to Congress under oath. RT, *Obama on Clapper's spy lie: 'He should have been more careful'* (Jan. 31 2014), available at http://rt.com/usa/obama-dni-clapper-lie-485/. He later apologized to committee chairperson Senator Dianne Feinstein, admitting that his response "was clearly erroneous—for which [he] apologize[d]." Clapper Letter to Sen. Feinstein, available at http://www.dni.gov/files/documents/2013-06-21%20DNI%20Ltr%20to%20Sen.%20Feinstein.pdf.

Senator Rand Paul told CNN "[t]hat Clapper is lying to Congress is probably more injurious to our intelligent capabilities than anything Snowden did." Jose DelReal, *Rand Paul slams James Clapper over NSA 'lying,'* Politico (Dec. 18 2013), available at http://www.politico.com/story/2013/12/rand-paul-james-clapper-national-security-agency-101306.html. Senator Paul added that, just as the Government Defendants' have continually demonstrated, "Clapper has damaged the credibility of the entire intelligence apparatus and [he is] not sure what to believe anymore when they come to Congress."[21] *Id.*

[21] Relevant to the points made herein, Senator Rand Paul also stated to CNN that "[i]f the intelligence community says we're not spying on Americans and they are, and then they say we're not

"It is now clear to the public that the list of ongoing intrusive surveillance practices by the NSA includes not only bulk collection of Americans' phone records, but also warrantless searches of the content of Americans' personal communications." Ron Wyden, Senator for Oregon, *Wyden, Udall on Revelations that Intelligence Agencies Have Exploited Foreign Intelligence Surveillance Act 'Loophole,'* Wyden (April 1, 2014), available at http://www.wyden.senate.gov/news/press-releases/wyden-udall-on-revelations-that-intelligence-agencies-have-exploited-foreign-intelligence-surveillance-act-loophole.

C. An Alleged Voluntary Discontinuation Of The Government Defendants' Illegal Government Surveillance Does Not Render Plaintiffs' Claims Moot.

Even if the Government Defendants discontinued their illegal government surveillance, which they most likely did not, the Government Defendants could, and most likely will, resume accessing Internet metadata and other data through Section 215 or some other vehicle, the Government Defendants have hung their hat on the slender stand of mootness, claiming that their decision to voluntarily cease the offensive conduct in 2011 is no longer capable of adjudication in this

---

collecting any data, it's hard to have confidence in them." Politico, *supra.*

Court. This Court must reject Government Defendants' argument. A defendant that simply ceases illegal conduct cannot avoid the consequences for it's past, present or future conduct. This is axiomatic and black letter law.

The Government Defendants' conceded that "at one time [the Government] acquired bulk Internet metadata . . . pursuant to FISA's pen/trap provision." Govt.'s Opp'n. Motion to Dismiss in *Klayman I* [Docket No. 74] at 15. "The data collected included certain routing, addressing, and signaling information such as 'to' and 'from' lines in an e-mail . . . and the date and time an e-mail [was] sent," but not the 'content of [an] e-mail [or] the 'subject' line. NSA collected large amounts of this transactional information from certain telecommunications service providers and analyzed it to obtain foreign intelligence information." *Id*. According to Government Defendants, "This [illegal government surveillance] of bulk Internet metadata [ ] was terminated in 2011, for operational and resource reasons." *Id.* at 16.

The Supreme Court has stated "[i]t is well settled that "'a defendant's voluntary cessation of a challenged practice does not

deprive a federal court of its power to determine the legality of the practice" for "if it did, the courts would be compelled to leave '[t]he defendant . . . free to return to his old ways.'" *Friends of the Earth v. Laidlaw Envt'l Services, Inc.*, 528 U.S. 167, 189 (2000) (*quoting City of Mesquite v. Aladdin's Castle, Inc.*, 455 U.S. 283, 289 (1982)); *see United States v. W.T. Grant Co.*, 345 U.S. 629, 632 (1953) (holding that "voluntary cessation of allegedly illegal conduct does not deprive the tribunal of power to hear and determine the case).

When the basis of mootness is voluntary cessation, "[a] case *might* become moot if subsequent events made it *absolutely clear* that the allegedly wrongful behavior could not reasonably be expected to recur." *Laidlaw*, 528 U.S. at 191 (emphasis added). Precisely because the voluntary cessation of allegedly wrongful activity can be undone by an equally voluntary decision to resume the conduct, courts have consistently held that "[t]he heavy burden of persua[ding] the court that the challenged conduct cannot reasonably be expected to start up again lies with the party asserting mootness." *United States v. Concentrated Phosphate Export Ass'n*, 393 U.S. 199, 203 (1968); *see also Laidlaw*, 528 U.S. at 189.

Here, it is more than a stretch to claim that government officials who did not follow the law before will suddenly follow the law now – especially when they refuse to acknowledge that their previous course of conduct was wrongful and are "certified" perjurers before Congress and the court.

In cases involving cessation of challenged conduct by Government officials, courts generally require that the cessation of the challenged conduct be accompanied by circumstances indicating the change is a genuine act of self-correction in order to find that the issue does not require adjudication. *See Magnuson v. City of Hickory Hills*, 933 F.2d 562, 565 (7th Cir. 1991); *see also* 13A Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure § 3533.7 (2d ed. 2004) (noting that while "[c]ourts are more apt to trust public officials than private defendants to desist from future violations . . . the tendency to trust public officials is not complete . . . nor is it invoked automatically.") Moreover, in *Armster*, the hold held that where the Justice Department did not concede that challenged conduct was illegal, bare assertion that it would not recur was insufficient to establish mootness because "[i]t has been long recognized that the likelihood of recurrence of challenged

activity is more substantial when the cessation is not based on a recognition of the initial illegality of that conduct." *Armster v. United States District Court for the Central District of California*, 806 F.2d 1347, 1359 (9th Cir. 1986); ("It has been long recognized that the likelihood of recurrence of challenged activity is more substantial when the cessation is not based on a recognition of the initial illegality of that conduct."). *Id*.

Thus, in light of well-established principles, the Government Defendants' argument that collection under PRISM "was discontinued in 2011", a mere three years ago, holds no weight. Government Defendants' can easily return to their old practice of collecting metadata – if Government Defendants' ceased the activity at all – through the PRISM illegal government surveillance and other similar illegal government surveillance.

Also, the fact that Plaintiffs have requested monetary damages in addition to injunctive relief also renders Plaintiffs' claims regarding the collection of metadata not moot. Plaintiffs are entitled to monetary damages for the harm caused during the period that the Government Defendants admit that they were collecting citizen's Internet metadata and other data through their illegal and unconstitutional surveillance.

Discovery is, at a minimum, necessary to determine the extent and amount of monetary damages that Plaintiffs are entitled in regards to the time period that the Government Defendants violated Plaintiffs' Constitutional rights.

The totality of the record shows that the Government Defendants have not discontinued the Section 215 illegal government surveillance, but even if they have, this does not moot out Plaintiffs' claims, particularly since Defendants concede that the illegal and unconstitutional conduct continued to occur within the applicable statute of limitations which is three years.

D. Plaintiffs Have Provided Sufficient Evidence To Show That The NSA Has Targeted Plaintiffs' Internet Data Content.

The District Court found that Plaintiffs made a sufficient showing that the Government Defendants targeted Plaintiffs' telephony metadata. For the very same reasons, Plaintiffs have sufficient evidence to show that the Government Defendants also collected their, and all Americans', internet metadata. In fact, the reality is that the same intrusion has occurred with regard to internet metadata as it has been shown with telephony metadata. Clapper's own responses and

revelations shows that the Government Defendants are still using both telephony and internet metadata of Plaintiffs and hundred of millions of American citizens.

For the aforementioned reasons, the District erred in denying preliminary injunctive relief to Plaintiffs in *Klayman II*.

III. THE COURT SHOULD REACH A DECISION ON PLAINTIFFS' FIRST AND FIFTH AMENDMENT CLAIMS.

Plaintiffs' First and Fifth Amendment claims, which have not been ruled upon, are just as important as Plaintiffs' Fourth Amendment claim, and thus, this Court should reach a decision regarding these claims. As the District Court ultimately found that plaintiffs have made a sufficient showing to merit injunctive relief on their Fourth Amendment claim, the District Court decided to not reach their other constitutional claims under the First and Fifth Amendments.

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 *Gibson v. Florida Legislative Investigation Committee*, the court ruled, "[t]he First and Fourteenth Amendment rights of free speech and free association

are fundamental and highly prized and 'need breathing space to survive." 372 U.S. 539, 892 (1963) (citing *NAACP. v. Button*, 371 U.S. 415, 433 (1963)). 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' overly broad and sweeping surveillance raises precisely the same harm. In light of his public advocacy in matters of public interests 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 do not simply fear the possible surveillance of the Government, Plaintiffs are aware of actual and proven surveillance—much more than enough to confer standing. *See* SA 38 ("[T]he NSA . . . collected metadata."). This Court has already found that the Government Defendants queried and reviewed Plaintiffs' metadata. SA 38-39 ("I find that Plaintiffs [ ] have standing to challenge the NSA's querying procedures . . . .Plaintiff's metadata—indeed *everyone's* metadata—is analyzed, manually or automatically . . . .").

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.

The ACLU also addressed 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. Due to the violations of Plaintiffs' First and Fifth Amendment rights, this Court should reach a decision pertaining to these Constitutional claims.

CONCLUSION

In sum, this Court must respectfully affirm the District Court's Order of December 16, 2013, preliminary 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.

Indeed, as Chief Justice Roberts also ruled, this violation of privacy of Americans ignited the American Revolution for which Americans laid down their lives to found a new nation free from government tyranny. Accordingly, this Court should not only affirm the District Court's Order of December 16, 2013 by ordering a preliminary injunction in *Klayman I*, as well as ordering a preliminary injunction *Klayman II*, but should also remand to the District Court to remove the stay of its preliminary injunction, because even one more day of this outrageous and unconstitutional government abuse cannot be countenance any longer. The Founding Fathers intended that the judiciary serve as a check to unbridled legal and unconstitutional behavior.

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. Plaintiffs want to preserve the status quo, which will ultimately not harm anyone. Plaintiffs and the American people thus look to you for their salvation.

Plaintiffs hereby respectfully request oral argument at the earliest practicable date.

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 Rule of Appellate Procedure 32(a)(5) and (6) because it has been prepared in 14-point Century Schoolbook, a proportionally spaced font.

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 13,977 words excluding the parts of the brief exempted under Rule 32(a)(7)(B)(iii), according to the count of Microsoft Word.

/s/ Larry Klayman
LARRY KLAYMAN, ESQ.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 13th day of August, 2014, I filed a true and correct copy of foregoing brief 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.

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